中文用户手册

由 美国 **Alt-N Technologies,**公司

中国区独家总代理

比特瑞旺集团软件事业部 协助翻译

www.qast.com

Alt-N Technologies 有限公司

MDaemon ® 中文版– 用户手册

MDaemon 是 美国 ALT-N TECHNOLOGIES 有限公司的一项产品.
1179 Corporate Drive West, Suite 103
Arlington, Texas 76006
电话 817.525.2005
传真 817.525.2019
www.altn.com

版权所有 © 1996 - 2005 Alt-N Technologies®. 保留所有权利。
MDaemon, WorldClient, 和 RelayFax 是 Alt-N Technologies® 的注册商标。

ALT-N TECHNOLOGIES 最终用户许可协议

本最终用户许可协议（《协议》）是您（“被许可方”）和 Alt-N Technologies（“许可方”）之间有关正在安装的 Alt-N 软件产品的法律协议，其中包括电脑软件、“在线”或电子文档（“软件产品”或“软件”）。

您一旦安装、复制或以其他方式使用“软件产品”，即表示您同意接受本《协议》各项条款的约束。如您不同意本《协议》中的条款，则您不可以安装或使用本“软件”。

ALT-N TECHNOLOGIES 软件许可

该“软件产品”受版权法和国际版权公约，以及其它知识产权和公约的保护。该“软件产品”只许可使用，而不出售。该“软件产品”包含产品文档、服务器应用程序，以及单独标识为“组件”的支持文件，并在此统称为“软件”。

授予许可

Alt-N Technologies 授予您（作为个体）一份单独、非排他性、不可转让的许可，供在单一计算机上或多台计算机上安装并执行单一“软件”实例，前题为该软件不会同时有两个或多个明显的实例同步运行。在不超过 30 天的一次性评估期之后，该“软件产品”必须向 Alt-N Technologies 注册并激活。有关如何注册并激活的说明可以查找产品文档或访问：http://www.altn.com 或 http://www.altn.cn。无法获得合法的注册码并激活它，或无法保密注册和激活码，均构成对本《协议》的违约。

如果您是一个实体，Alt-N Technologies 授予您指定组织内的个人使用并管理该“软件”的权利，前题条件与个人用户遵守的限制相同。

任何回避该“软件”30 天试用限制或激活宽限期的行为，均构成对本《协议》违约。

使用该“软件”的 beta 版本或其它不用于向广大公众发布的版本，将严格限于 MD-BETA 测试社区的授权成员。

该“软件”不能用于传播“大量未经请求的商业电子邮件”（通常称为“垃圾邮件”）。为本节描述方便，“大量未经请求的商业电子邮件”应定义为包含产品或服务广告的电子邮件，发送至 50 个以上地址，而收件人没有明确表示接收此类电子邮件的意向。

禁止反向工程、反编译或反汇编该“软件产品”。

Alt-N Technologies 有权定期验证未发生违背该《协议》的条款的行为。

著作权

本“软件产品”内和相关的所有标题和版权都归 Alt-N Technologies 及其供应商所有。该“软件产品”受版权法和国际公约条款的保护。因此，必须如同对待任何其它有版权的资料一样对待该“软件产品”，除非：您可以(a)复制一份该“软件产品”仅用于备份或归档，或(b)在一台电脑上安装该“软件产品”，前题为保留原件的目的仅为备份或归档。禁止复制伴随该“软件产品”的印刷资料。本“软件产品”（包括但不限于本“软件”中所含的任何图像、照片、动画、录像、录音、音乐、文字和附加程序）、随附的印刷材料、及本“软件”的任何副本的产权和著作权，均由 Alt-N Technologies 拥有。您必须在本“软件”的所有副本上包含所有的版权标识。

第三方组件许可条款

设计为与该“软件产品”集成的第三方工具、应用程序和/或组件，必须取得 Alt-N Technologies 的许可。

免责声明

使用该软件提供商业性的邮件服务将需要获得另外的许可或替换许可条款。了解更多相关信息，请联系：xsp-license@altn.com。

上述担保，无论是明示或暗喻的，为担保的全部内容，包括对特殊应用目的的商品性和适应性担保。在适用法律所允许的最大范围内，ALT-N TECHNOLOGIES 或其任何代理商、

销售人绝不就因使用或不能使用本“软件”所引起的或有关的任何间接的、意外的、直接的、非直接的、特殊的、惩罚性的或其它任何损害赔偿（包括但不限于因人身伤害或财产损坏而造成的损害赔偿，因利润损失、营业中断、商业信息的遗失而造成的损害赔偿，因未能履行包括诚信或相当注意在内的任何责任致使隐私泄露而造成的害赔偿，因疏忽而造成的损害赔偿，或因任何金钱上的损失或任何其损它损失而造成的损害赔偿）承担赔偿责任，即使 ALT-N TECHNOLOGIES 或其任何代理商、销售人事先被告知该损害发生的可能性。即使补救措施未能达到预定目的，本损害赔偿排除条款将仍然有效。

本《协议》受中华人民共和国法律和国际公约的保护。

本许可协议如与英文版 EULA 之间存在任何歧义，以英文版为准。

章节列表

MDaemon® ____ **16**
MDaemon 的主界面 ____ **27**
主域配置 ____ **33**
次域 ____ **62**
远程配置 ____ **66**
WorldClient 服务器 ____ **72**
LDaemon/地址薄选项 ____ **96**
共享文件夹**/**邮件队列 ____ **102**
安全特性 ____ **112**
邮件头转换 ____ **186**
IP 缓存与 **DNS** 查询 ____ **189**
事件计划与拨号 ____ **192**
DomainPOP 邮件收集 ____ **205**
内容过滤器与反病毒 ____ **218**
邮件优先权 ____ **239**
日志选项 ____ **241**
系统服务设置 ____ **249**
其它选项 ____ **251**
管理 **MDaemon** 账户 ____ **271**
账户编辑器 ____ **284**
导入账户 ____ **308**
地址别名 ____ **313**
自动回复与 **MBF** 文件 ____ **318**
邮件列表 ____ **326**
目录 ____ **349**
域网关 ____ **351**
队列与统计管理器 ____ **366**
其它的 **MDaemon** 功能 ____ **371**

目录

第一部分....15
MDaemon 的主要性能....15

第一章 16

MDaemon® 16

简介....16
MDaemon 标准版和专业版 16
MDaemon 功能....16
在 MDaemon 中文版 8.1 中，哪些是新功能?....18
域名密钥（DomainKeys）邮件识别技术....18
灰名单....18
MDaemon V8 的新功能....19
改良的协作支持(仅限 MDaemon PRO) 19
WorldClient 的功能增强 19
Outlook Connector 集成和改良 19
安全性能增强....19
DomainKeys....19
改良的 AntiVirus 集成....20
增强的反垃圾邮件性能....20
增强的垃圾邮件过滤器....20
改良的垃圾邮件过滤引擎....20
支持 HashCash “Proof-of-work”....20
支持 WebAdmin 3.1 21
改良的队列管理....21
改良的错误管理....21
为网关用户验证提供的增强的 LDAP 查询 21
支持用户订制插件....22
其它功能和改进....22
升级到 MDaemon 8....22
Version 8.1.0 特别备注....22
Version 8.0.3 特别备注....23
Version 8.0.0 特别备注....23
安装....26

第二章 27
MDaemon 的主界面....27
统计和工具....27
消息与事件跟踪....28
组合日志查看....29
托盘图标....30
锁定/解锁 MDaemon 主界面....30

连接窗口......31
MDaemon 的 SMTP 工作流程......32

第三章......33
MDaemon 的主域配置......33
域配置编辑器......33
域......35
发送......37
POP 检查......39
重试配置......39
端口......42
DNS......44
计时器......47
线程......49
出列......51
On-Demand 邮件传递（ODMR）......52
出列 AUTH*......53
存档......54
修剪......56
预处理......58
未知邮件......60

第四章......62
次域......62
运行多个域（仅限 MDaemon 专业版）......62
次域编辑器......63
添加次域......65
编辑次域......65
移除次域......65

第五章......66
远程配置......66
WebAdmin......67
在 IIS 下运行 WebAdmin......68
WebAdmin SSL......71

第六章......72
WordClient 服务器......72
概述......72
日历和日程系统......72
ComAgent......73
ComAgent 的即时消息系统......74
自动地址薄同步......75
使用 WorldClient......76

启动 WorldClient 76
登入到 WorldClient 76
改变 WorldClient 的端口设置 76
WorldClient 文档 76
客户端帮助 76
WorldClient 邮件 77
WEB 服务器 77
在 IIS 下，运行 WorldClient 79
WorldClient SSL 80
WorldClient 的日程表 81
RelayFax 84
选项 86
Outlook Connector for MDaemon 90
Outlook Connector 用户 90
Outlook Connector 选项 92
附件链接 93

第七章 96
LDaemon/全局地址薄 96
LDaemon 97
LDAP 选项 99

第八章 102
共享文件夹/邮件队列 102
共享 IMAP 文件夹 103
共享文件夹 103
公共文件夹 105
访问控制列表 107
邮件队列 109
保持队列 110
还原 111

第九章 112
安全功能 112
安全特性 112
DNS 黑名单 (DNS-BL) 113
DNS-BL 选项 114
为每一个账户自动生成一个垃圾邮件文件夹和规则 115
DNS-BL 主机 116
删除 117
通知 117
在首次主机匹配时停止主机查询 117
发送匹配“邮件”而不是 “未知用户” 117
缓存 118

白名单列表......120
垃圾邮件过滤器......121
垃圾邮件过滤器......122
启发式......124
贝叶斯......126
贝叶斯高级选项......129
报告......131
HashCash......133
例外列表......135
白名单（自动）......136
白名单（收件人）......138
白名单（发件人）......139
黑名单......140
SSL 和证书......141
电子邮件 SSL......142
WorldClient SSL......144
WebAdmin SSL......147
创建和使用 SSL 证书......149
创建一个证书......150
导出 MDaemon CA 证书......150
使用由第三方 CA 发行的证书......150
地址抑制......152
IP 屏蔽......154
主机屏蔽......156
IP 防护......158
SMTP 认证......160
SMTP 之前先 POP......162
站点策略......163
创建一个 SMTP 连接策略声明......163
中继设置......164
可信的主机......166
Tarpit 设置......168
反向查询......171
局域网 IPs......174
灰名单......175
发件人策略框架......178
域名密钥和 DomainKeys 邮件识别技术......180
加密签名......181
加密校验......183

第十章......186
报头转译......186
报头转译......186
报头转译例外......187

第十一章....189
IP 缓存和 DNS 查询....189
IP 缓存....189
DNS 查询....191

第十二章....192
事件调度和拨号....192
事件调度....192
发送/接收邮件....192
简易调度....193
AntiVirus 更新....194
反垃圾邮件更新....196
RAS 拨号设置....198
拨号设置....198
ISP 登录设置....200
投递连接....202
局域网域名....203
局域网 IP....204

第十三章....205
DomainPOP 邮件收集....205
DomainPOP 邮件收集....207
帐号....207
分析....209
处理....211
路由规则....212
外来邮件....214
安全....215
名称匹配....216

第十四章....218
内容过滤器和 Anti-Virus....218
内容过滤器编辑器....219
创建新的内容过滤器规则....221
调整存在的内容过滤器规则....224
在你的过滤器规则中，使用规则表达....224
管理/附件....228
文件压缩....229
AntiVirus....231
AntiVirus 更新程序....233
通知....236
邮件宏....237

第十五章....239

优先级邮件......239
　　优先级邮件......239

第十六章......241
日志......241
　　日志模式......241
　　　　维护......243
　　　　事件日志......245
　　　　选项......246

第十七章......249
系统服务设置......249
　　服务设置......249
　　网络资源访问......250

第十八章......251
其他选项......251
　　界面......251
　　服务......254
　　邮件头......256
　　修正......259
　　系统......260
　　磁盘......262
　　MultiPOP......264
　　WAB......266
　　杂项......267

第二部分......270
MDaemon 的帐号功能......270

第十九章......271
管理 MDaemon 帐号......271
　　帐号数据库选项......272
　　　　ODBC Selector 向导......273
　　　　　　转移你的帐号数据库到 ODBC 可访问存储......273
　　　　　　创建新的系统数据源......275
　　帐号管理......277
　　　　创建 MDaemon 用户帐号......278
　　新建帐号默认值......279
　　　　帐号默认值......279
　　　　　　模版宏......280
　　　　Web 访问默认值......281

第二十章......284
帐号编辑器......284
帐号编辑器......284
帐号......284
邮箱......286
转发......288
选项......290
管理员......292
配额......293
限制......295
外发邮件限制......296
Web......297
自动回复......299
IMAP 邮件规则......301
MultiPOP......303
共享文件夹......305
访问控制列表......306

第二十一章......308
导入帐号......308
从文本文件中导入帐号......308
Windows NT 安全帐号整合......310
NT/2000 帐号导入器......310
NT/2000 服务器属性......310
帐号导入......311
导入选项......311

第二十二章......313
地址别名......313
别名......314
选项......316

第二十三章......318
自动回复与 MBF 文件......318
自动回复......318
帐户......318
自动回复......319
例外列表......321
选项......322
创建自动回复脚本......322
自动回复脚本例子......323

第三部分......325
附加的 MDaemon 的功能......325

第二十四章......326
邮件列表......326
邮件列表编辑器......326
创建新的邮件列表......326
修改现有的邮件列表......326
选项......327
成员......329
增强列表修改......330
路由......331
ODBC......333
为邮件列表选择和配置一个 ODBC 系统数据源......334
创建一个新的系统数据源......336
订阅......338
订阅邮件列表......339
支持文件......341
通知......342
安全......344
摘要......346
公共文件夹......348

第二十五章......349
目录......349
编录编辑器......349
公共编录......350

第二十六章......351
域网关......351
网关编辑器......352
自动网关创建......353
网关......354
ETRN......355
ATRN......357
选项......359
POP/IMAP......360
限额......361
LDAP......362
对 LDAP 验证队列使用多重配置......363
自动创建网关......364

第二十七章......366
队列与统计管理......366

队列页......367
选择文件......368
用户页......370
日志页......372
报告页......374
定制队列与统计管理......375
MDstats.ini File......375
MDStats Command Line Parameters......376

第二十八章......377
带宽限制......377
带宽限制......378
局域网域名......380
局域网 IP......381
签名文件......383
签名文件......383
MDaemon 的文字编辑器......384
编辑 MDaemon 文件......384
RAW 邮件说明 v3.1......385
RAW v3.1 支持的特别领域......386
通过电子邮件远程控制服务器......387
帐号的访问和控制......387
邮件清单和分类控制......388
通用邮件控制......390
MDaemon 和代理服务器......391
其它信息......391

第一部分

MDaemon ® 中文版

MDaemon 的主要性能

第一章

MDaemon ® 中文版

MDaemon®

在 Windows 系统下的多用途邮件服务器

简介

MDaemon Server v8 是一个基于标准 SMTP/POP/IMAP 协议并提供全部邮件服务功能的邮件服务器软件。Mdaemon 定位于管理任何个人用户的邮件需求和要求，包括一套强大的整合工具，以便于管理账户和邮件格式。Mdaemon 提供了一套可扩展的 SMTP、POP3、和 IMAP4 邮件服务器，其中包括 LDAP 支持、一套整合的基于浏览器的邮件客户端，内容过滤器、垃圾邮件拦截器、广泛的安全性能，以及更多。

MDaemon 标准版和专业版

ALT-N TECHNOLOGIES 的 MDaemon 服务器有两个有效版本：MDaemon 标准版和专业版。通过 MDaemon 标准版强大的性能，您可以从一个独立的 ISP 提供的 POP3 账户上收取您的网络邮件，或者使用 MDaemon 完善的 SMTP 服务器创建一个完全的域。通过 增强功能的 IMAP4 和多域支持，MDaemon 专业版是一个理想的针对企业级机构的电子邮件中枢。MDaemon 专业版也增加了组日历和日程安排，一个即时消息系统，对 WorldClient 的多语言支持，域网关的自动创建，以及比标准版更为广泛的功能。对于 MDaemon 标准版和专业版的区别的讨论，请参见“*MDaemon Versions: Comparing Standard and Pro*”白皮书。这份白皮书和其他有用资源可以登录我们的网站下载。www.altn.com

MDaemon 功能

除 SMTP, POP, 和 IMAP 邮件处理之外，MDaemon 还具备其他许多功能。以下就是功能中一些较具代表性特征的列表：

- MDaemon 强大的处理能力使得在整个局域网中提供像拨号登陆 POP3 邮箱一样的邮件服务成为了可能。同样，为整个网络提供电子邮件的服务费用比正常关联的费用减少了很多。
- 通过 MDaemon 的反病毒功能可以对病毒的扫描和保护起到全面的支持。这一功能提供了有效的反病毒保护。在到达指定收件人之前，通过检测，邮件中的病毒可以被自动清除或者删除掉。而且，您可以配置 MDaemon，使得 MDaemon 发送有关感染邮件的信息给管理员、发件人和收件人以提醒他们对病毒引起注意。MDaemon 的反病毒功能是作为一个单独许可的产品，这个产品可以从 www.altn.com上获得。
- MDaemon 服务器 v8 提供一套完整的邮件列表或者邮件组管理功能的解决方案，这些功能由支持无限数量的包含本地和/或远程成员的独特分布构成。列表可以被设置成允许或者拒绝订阅、公共的或者私人的，发表回复到列表中的每个人或者此邮件的创作者，也可以以摘要格式发送，以及配置使用其他的众多功能。
- WorldClient 是一套 MDaemon 的整合组件。这个令人激动的产品使您的用户可以选用他们

自己喜欢的网络浏览器而不是工作站中的独立邮件客户端来访问他们的邮箱。这个工具对于那些没有固定电脑的移动人员和用户来说，是一个完美的接收邮件的解决方案。

- WorldClient 配备了一整套的邮件服务器功能。收发邮件、邮件拼写检查、在多个个人文件夹中管理您的邮件，可以从18种语言中任选一种来显示介面，通过组日历和日程表功能来安排会议和约会，管理您的 MDaemon 账户设置（当使用 WebAdmin 协助时），管理联系人等等。WorldClient 也配置了 ComAgent，一个小工具，可以被下载并安装到用户的本地机器上。这个软件可以使用户不用打开网络浏览器就可以轻松的进入自己的邮箱、文件夹以及检查是否有新邮件。同时，它也提供一套完整的即时消息系统，可以被用来与其他 MDaemon/WorldClient 用户快捷的“聊天”。
- MDaemon 拥有很多功能被用来帮助您确保您账户的安全。垃圾邮件过滤器和DNS黑名单功能能帮助您终止那些垃圾邮件发送者企图间接或直接发送到您域里面的垃圾邮件。IP 和 Host 屏蔽以及地址屏蔽功能可以阻止某些域和地址连接或者通过您的系统发送邮件。以上这些功能使得在屏蔽所有其他 IP 的同时，允许连接特定的 IP 成为可能。
- 配置了对轻量级目录访问协议(LDAP)的支持, MDaemon 能使您的 LDAP 服务器保持和它的账户用户同步。您可以用它来保持一个LDAP 地址薄更新，以使得支持 LDAP 的邮件客户端的用户能够访问。您可以选择使用您的 LDAP 服务器作为 MDaemon 账户数据库替代 ODBC 访问数据库或者本地的 USERLIST.DAT 系统。这样，您可以设置多个 MDaemon 配置在不同的位置共享相同的账户数据库。
- MDaemon 可以被设置使您的 Windows 地址薄或者 Microsoft Outlook 联系人随时保持与您的用户信息保持同步。这一功能为您的用户提供了制作全局地址薄的另外的方法。
- 地址别名提供通过对一个虚构的邮箱中发送邮件到一个有效的账户或者邮件列表中去。这使得一个个人账户或者列表在一个或者多个域里面拥有多邮件地址成为可能。
- 域网关功能提供可以为您在本地网络或者位于 Internet 位置的各种不同的部门和组设置独立域的选项。利用这些功能，由 MDaemon 作为网关的域内的所有邮件地址都将被放到域内的邮箱。之后，可以被域内 MDaemon 服务器或者邮件客户端收集和分发给域内的用户。
- 通过使用特殊格式的电子邮件消息，用户可以远程控制账户。这个功能提供更好的管理上的灵活性，并授权把日复一日的简单账户维护任务转移给用户，例如修改密码等等。
- 支持 WebAdmin.。这是一个免费的基于WEB的远程管理程序，可以从 www.altn.com 的网站上获得。它完美的整合了 MDaemon 和 WorldClient，使得您的用户可以通过他们自己的浏览器查看和编辑他们的账户。您可以指定您的用户可以编辑那些设置，也可以在基于每个账户分配访问许可。WebAdmin 可以被管理员（以及任何您允许的用户）用来查看或者编辑任何的 MDaemon设置，任何您通过 WebAdmin 设置成允许被访问的文件。
- 利用文件目录，邮件管理员可以创建密码保护的可加密的文件组，并且可以通过使用特殊的邮件格式自动的发送他们。
- 邮箱账户格式主要是使用邮箱格式文件（MBF），一个具有广泛邮件系统兼容性的文件格式。
- 一套内部消息传送系统－RAW 邮件，提供一种简单方法来将消息放入到邮件流当中去，并且极大的简化了自定义邮件软件的开发。使用 RAW，一个完整的邮件系统可以设计成只使用简单文本编辑器和几个批处理文件。
- 内容过滤系统使得您基于来信和发信自定义服务器行为成为可能。您可以插入并且删除邮件头、为信件添加注脚、移除附件、路由副本到其他用户、发送一个即时消息发送到某个人、运行其他程序，以及更多。

在 MDaemon 中文版8.1中，哪些是新功能?

域名密钥（DomainKeys）邮件识别技术

MDaemon 8.1支持最新的DomainKeys Identified Mail (DKIM)技术，这是电子邮件加密签名和验证未来的发展发向。基于Yahoo!的域名密钥（DomainKeys）技术和Cisco的Identified Internet Mail，DKIM能为您的用户提供全新层面的保护，帮助保护防止网络诈骗和其它类型的来自email网页伪造的攻击威胁。Alt-N Technologies一直直接与行业先驱并肩作战，如Yahoo!，Cisco，IBM，Sendmail等，共同开发DKIM规范，并且目前它已经成为www.ietf.org上的一个IETF互联网草案。针对DKIM标准化的讨在2005年7月31日法国巴黎召开的第63届IETF会议上展开。
DKIM是DomainKeys的一个扩展集，尽管它将其签名信息放置在一个不同的邮件标题中。 使用DomainKeys的签名者将使用一个指向某个DomainKeys关键记录的DomainKeys签名，以及一个生效器来检查DomainKeys签名是否符合DomainKeys规则。DKIM将其签名信息放置在一个不同的邮件标题中，它将指向一个DomainKeys关键纪录或一个DKIM关键纪录。生效器检查DKIM签名是否符合DKIM规则并将使用签名中引用的关键纪录。这是DKIM设计中一项重要的战略成就，因为它与现存的DomainKeys基础构造兼容。DKIM维护句法和句法与DomainKeys管理公开关键纪录的配置基础的兼容性。这意味着当验证过程发展并包含DKIM时，用户不需要改变其现有的关键纪录。DKIM和DomainKeys都从包含在位于Security SPF/DomainKeys & DKIM…的SPF，DK&DKIM对话框中的密码签名/验证标签中进行配置。
更多关于DKIM的信息，请见www.ietf.org上的互联网草案，以及Alt-N Technologies新闻发布：http://www.altn.com/press/press_release.asp?ReleaseID=137

灰名单

从安全菜单中进行配置(位于“安全”—>“中继/…/灰名单… ”—>“灰名单”)，灰名单是一项反垃圾邮件技术，它利用了SMTP服务器重新发送任何收到临时出错代码（如“稍后再试”）的邮件。通过这项技术，当从一个非白名单列表或先前未知的发件人的邮件到达服务器时，在SMTP进程中它会被灰名单拒绝并收到一个临时出错代码。而且，在一段指定的时间内（如，30分钟），任何重新发送的尝试将被临时拒绝。 因为垃圾邮件发送者在邮件被拒绝后通常不会重新发送。灰名单能帮助显著减少您的用户收到垃圾邮件的数量。即使垃圾邮件发送者企图在后来重新发送邮件，很可能那时垃圾邮件发送者已经被成功识别并且被其它反垃圾邮件选项(如，DNS黑名单)成功地阻止。值得注意的是，这项技术也会同时延缓某些正常邮件的接收。但是，合法邮件还是会在定义的灰名单时间段失效后被重新发送。
更多关于灰名单的概要，请访问Even Harris的网站：
http://projects.puremagic.com/greylisting/.

MDaemon V8的新功能

改良的协作支持(仅限MDaemon PRO)

WorldClient的功能增强

对MDaemon和WorldClient协作的支持被广泛地改进。从WorldClient，您现在能方便地创建预约，确定会议时间，访问地址簿。连续预约现在已经被全面支持，并且预约拥有更多的描述字段而变得更加强大。而且，联系人，日历，和任务数据现在被作为IMAP文件夹存储在每个用户的邮件根目录中。通过WorldClient，您的用户能访问这些个人文件夹和控制其他用户的访问权限。所有WorldClient的主题(尤其Lookout)都已经运用了新的模板，用更加合理和引人注目的方式来显示联系人，日历，和任务文件夹。全域联系人，日历和任务文件夹现在能被自动创建。这些都是公共文件夹，所有该域的用户都将通过WorldClient来访问它们。默认情况下，所有该域的用户都能添加，编辑和删除这些文件夹中的项目，您也能从位于共享文件夹菜单中的选项来轻松改变这些权限

Outlook Connector集成和改良

用户通过WorldClient访问所有最新的系统协作功能。然而，由于系统是完全基于IMAP/ACL之上的，所有数据存储为XML和RFC/TNEF格式，这允许可以与Outlook Connector for MDaemon (原先的GroupWare for MDaemon)无缝集成，另一个Alt-N Technologies开发的独立授权的产品。当您安装了Outlook Connecter for MDaemon，用户就能通过安装一个很小的Outlook Connector插件通过Microsoft Outlook访问所有的协作功能，这个小插件可以从WorldClient内部下载得到或通过其他途径分发得到。MDaemon现在在其主界面中包含了一个Outlook Connector标签，显示了所有MDaemon邮件服务器和Outlook Connector客户端之间的IMAP交互活动。此外，新的Outlook Connector关联日志选项已经被添加到日志菜单中。您现在能维护一个单独的日志文件，它将跟踪所有服务器与Outlook Connector客户端之间的IMAP活动，您还能指定是否集成的日志窗口该包含Outlook Connector活动。

更多关于Outlook Connector的信息，请访问www.altn.com 。

安全性能增强

DomainKeys

域名密钥（DomainKeys）是一个email验证系统，能用于防止email地址欺诈。而且，因为大多数的垃圾邮件都包含欺骗性的地址，DomainKeys能帮助从很大程度上减少垃圾邮件，尽管它不是专门设计用于反垃圾邮件的工具。最后，DomainKeys还能用于确保收到的邮件的完整性，或确保邮件在发件服务器被发出直到到达接收服务器的过程中未曾受到篡改。换句话说，有了DomainKeys系统，收件服务器就能确信到达的邮件是来自发件人的并且没有人用任何方式改变过邮件信息。为了确保邮件的有效性和完整性，DomainKeys使用一个公钥和私钥对。一个加密的公秘钥被发布到发送服务器的DNS记录，然后每个发出的邮件都被服务器用相应的秘匙作了标记。对于收到的邮件，当收件服务器发现一个邮

件被作了签名，它将从发件服务器的DNS记录中找回公钥，然后将其与邮件中的签名比对来确定邮件的合法性。如果收到的邮件不能通过验证，那么收件服务器就知道其包含了伪造的地址或曾被篡改。失败的邮件可以被拒收，或者被接收但是会调整其垃圾邮件的打分。
更多关于DomainKeys的信息，请访问：http://antispam.yahoo.com/domainkeys 。

改良的AntiVirus集成
MDaemon现在能在SMTP进程中对收到的邮件扫描病毒，而不是等待进程结束再扫描。因为在Mdaemon收件服务器正式接受邮件和结束进程之前，每个收到的邮件都会被扫描，发件服务器仍然对此负责-邮件还没有从技术上被递送完成。因此，在发现病毒后，邮件就能被拒绝。而且，因为邮件被拒绝了，没有更进一步的防病毒操作将被实施。没有隔离或清除程序将被执行，并且没有任何通知信息将被发送。这能很大程度地减少感染邮件的数量和您以及您的用户收到的病毒报告邮件的数量。这个功能会减缓SMTP服务器的处理速率。

增强的反垃圾邮件性能

增强的垃圾邮件过滤器

默认情况下，MDaemon在SMTP进程中将对所有的邮件执行垃圾邮件过滤扫描来确定是否这些邮件的垃圾邮件打分超过了阀值而被拒绝。对于被接受的邮件，MDaemon将执行另一个基于队列的扫描并根据各个邮件的打分和您的垃圾邮件过滤设置分别处理这些邮件。从垃圾邮件过滤对话框中启发式标签上的一个新的选项，您现在能配置MDaemon来省略这个基于对列的扫描并将最初垃圾邮件扫描的结果作为最终结果。这能显著减少CPU的使用并增加反垃圾邮件系统的效率。然而，当基于队列的扫描被省略时，仅有默认SpamAssassin邮件标题将被添加到邮件中。如果您曾对默认SpamAssassin邮件头或在您本地.cf文件中的特定的定制邮件头进行过任何修改，那些改动将被忽视。

*版本**8.0.3**的新特性*

改良的垃圾邮件过滤引擎

MDaemon的垃圾邮件过滤引擎已经被升级到SpamAssassin 3.0。这个全新版本的SpamAssassin包含了众多升级和改进。
完整的改进列表，请访问http://www.spamassassin.org。

支持HashCash “Proof-of-work”
HashCash是一项“proof of work”系统，它既是一个反垃圾邮件工具也是一个类似于电子邮票的拒绝服务对策。使用了HashCash系统，MDaemon能制造HashCash邮票，他的作用并不在于实际的邮资，而是耗费一定的CPU处理时间。一个HashCash邮票被插入到一个被发出的邮件标题中，然后被收件人的邮件服务器验证并根据邮票值分别权衡。被加上邮票的邮件更可能被认为是合法的并通过收件人的服务器的反垃圾邮件系统。使用HashCash邮票能帮助减少错误并防止邮件由于未能通过一个文字过滤器或黑名单系统而被错误地拒绝。
更多关于HashCash的信息，请访问http://www.hashcash.org/。

支持WebAdmin 3.1

MDaemon不再支持WebAdmin 3.1之前的版本。您可以从如下地址免费下载获得最新版本的WebAdmin：http://www.altn.com/WebAdmin/。

改良的队列管理

MDaemon的主界面现在包括一个基本的队列管理系统。它用一种更完整的样式模拟一些队列和统计管理功能。双击该统计面板中的一个队列现在就会将主面板转换成这个新队列管理系统，而不是打开队列和统计管理器。然而，您还能通过双击一个队列并用队列和统计管理器来浏览它，如果您选择这么做的话。

改良的错误管理

MDaemon现在包含了一个保持（Holding）队列。这个新的队列能被用于接收那些在防病毒，反垃圾邮件或内容过滤进程中会导致软件异常的邮件。如果在处理一个邮件时发生某个软件错误，这个邮件将被转移到holding队列中并不被发送。被放置到holding队列中的邮件将留在其中直到管理员采取措施来将它们移走。在主用户界面上有一个*处理holding队列* 按钮，在队列菜单上也有一个同样的选项。您也能通过在主界面上右击holding队列然后从右击菜单中选择“重新排队”来处理这些邮件。处理holding队列将移动所有的邮件到远程或本地队列用于正常的邮件处理。如果引起邮件发生错误的原因依然存在，那么在发生错误时邮件将被重新放回holding队列中。如果您想尝试发送holding队列中的邮件而忽略任何可能发生的错误，那么您可以通过在主界面上右击holding队列并从右击菜单中选择“释放”来实现。当从holding队列中释放邮件时，将会打开一个确认框来提醒您这些邮件可能包含病毒或者它们不能够在防病毒，反垃圾邮件或内容过滤进程中正确的过滤。

为网关用户验证提供的增强的LDAP查询

当使用LDAP查询来验证域网关用户时，您现在能为您的网关域指定多重LDAP配置。为了指定额外的LDAP参数集，正常设置您的第一个参数集，然后使用记事本手动编辑GATEWAYS.DAT文件。您的新的参数集可以使用如下格式来创建：

```
LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
LDAPRootDN1=<root DN>
LDAPObjectClass1=MDaemonContact
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

对每一个全新的参数集，给每个参数名上的数字值加1。例如，在上述样例中，

每个参数名都以“1”结尾。如果创建另一个参数集，每个参数名必须以“2”结尾。在另一个参数集中，每个参数必需以“3”结尾，以此类推。
当LDAP查询发生时，MDaemon将依次执行多重LDAP查询来寻找匹配。 如果发生错误或找到匹配，不会执行进一步的检查。

支持用户订制插件

MDaemon现在包含了一个用于集成用户订制插件的系统。这使得将用户应用程序直接集成到MDaemon图形用户界面并嵌入到MDaemon的邮件处理链中变成可能。您的应用程序将作为MDaemon界面的一部分出现，而且它处理邮件时不会对MDaemon引发问题。

更多关于MDaemon插件的信息，请参见`\Docs\Api\Plugins.txt`。

其它功能和改进

参见`Relnotes.txt`文件，它位于MDaemon的`\Docs\`子目录中。它包含了

MDaemon从上个版本升级到该版本包含的所有新功能特性，改变和修正的列表。

升级到MDaemon 8

下面是当您执行从早期版本升级到MDaemon 8的操作时，您可能需要知道的特别备注列表。

Version 8.1.0特别备注

· 下列条目将被自动添加到您的Tarpit白名单文件中(`NoTarpit.dat`)：

```
127.0.0.*
192.168.*.*
10.*.*.*
172.16.0.0/12
```

· 默认的最新安装将给SPF和DomainKeys“通过”结果打分-0.5。之前，这个分数

是-2.5，这个分数被认为太多。推荐对于现有的安装，您检查并改变这些分值。

· DomainKeys签名文件(`DKSign.dat`)的格式已经改变。如果您在这个文件中指

定选择器，您现在必须稍微改变一下方式。用记事本打开`DKSign.dat`文件，并

阅读文件顶部的文本来获知如何使用“S=”来指定您的任意的选择器，如何使用全新的“d=”来指定一个签名域。

Version 8.0.3特别备注

•下列条目将被自动添加到您的SPF白名单文件(SPFXcpt.dat)以及DomainKeys验证白名单文件(DKVerifyXcpt.dat)中：

```
127.0.0.*
192.168.*.*
10.*.*.*
172.16.0.0/12
```

•您的SpamAssassin local.cf文件的一个条目被改变了。如果在您的local.cf文件中有“dns_available yes”，这一行已经被移除。移除它致使SpamAssassin在尝试使用那些依靠它的规则前首先检查DNS是否可用。这是一个聪明的选项，但未能创建额外的负载，因为测试DNS连通性可能不是对所有站点都有必要。如果您想改变这个设置或完全禁止基于DNS的规则条目，您可以通过使用位于垃圾邮件过滤对话框上的垃圾邮件过滤标签中最新的“DNS是否可用？”来实现。

• 默认情况下，MDaemon将在SMTP进程中对收到的邮件执行垃圾邮件过滤扫描。如果邮件分值超过12.0，这个邮件就不会被接受。您能改变这个极限到任何您觉得合适的数值，只要使用位于垃圾邮件过滤对话框上启发式标签中的*“SMTP拒绝分值大于或等于该分值的邮件”*选项就可以实现。将该值设置成“0”将完全禁止基于SMTP的扫描。

Version 8.0.0特别备注

• MDaemon 8.0包含了一个产品激活系统来帮助反盗版和保护合法用户的利益。当MDaemon启动后，它将立即启动激活向导，引导您完成一个简单的一次性的进程来激活您的注册码。您能通过一个自动的在线进程进行快速激活或通过一个安全的web站点手动完成。激活进程验证您正在使用的注册码是否合法，它将获取您的注册信息，安装MDaemon的计算机的信息，以及您的网卡MAC地址。这使得他人无法非法使用您的注册码。只有在您更换了网卡后，您才需要进行重新激活操作。点击帮助→激活您的注册码… 菜单选项来运行激活向导。多重激活是允许的(例如当您重新安装MDaemon，将其移动到一个不同的计算机上，改变

您的网卡，等)，但这仅为了给用户提供方便，而不能违背EULA或企图同时在不同的机器上使用相同的key。

注意: 在整个激活过程中不需要获取及传递任何您的个人信息，注册用户有30天来激活软件，为了让MDaemon 8.0正常工作，激活操作是必需的。

更多关于激活的信息，参见：

`http://www.altn.com/Activation/faq.asp`

· 为了支持MDaemon最新的协作系统，每个用户的日历、联系人和任务文件夹在安装过程中被创建。每个域也会创建一个联系人文件夹。如果任何这些文件夹已经存在，他们将被重新命名为`Old Calendar`，`Old Contacts`，和`Old Tasks`，而且当文件夹被重命名时，访问控制被保留。此外，地址簿和日历格式已经改变。因此，安装进程将自动转换每个用户邮件根目录下的的私人地址簿文件(`addrbook.xml`) 到新的联系人文件夹，而且日历信息将在日历文件夹内从原来的`Calendar.mrk`文件移植到新的XML格式。对于域公共地址簿，每个都将被转换并放置到域的联系人公共文件夹。在这个进程中，没有任何一个原始文件会被删除。您不必重复该转换/移植进程，但如果有必要的话，您可以运行`\MDaemon\App\MD3Conv.exe`来为任何用户（或所有用户）移植日历和联系人数据。

· MDaemon不再保持一个单一的可被所有域访问的全球地址簿。地址簿现在基于单个域进行维护。如果您想创建一个全局地址簿或任何其它地址簿，您可以通过共享文件夹对话框的公共文件夹标签来实现。

· MDaemon现在包含SpamAssassin 3.0。这个新版本的SpamAssassin包含了众多升级和改进。这些改进的完整列表，参见：http://www.spamassassin.org。

· 在垃圾邮件过滤对话框的启发式标签中，指出是否邮件标题标签将被包括在垃圾邮件中的方法已经改变。SpamAssassin不再支持选项来打开或关闭标题修改。而是，邮件标题标签的存在决定了用还是不用。因此，请检查这个标签并确定标题修改是按照您喜欢的方式。而且，在SpamAssassin 3中的`_HITS_`标签并不为分值加上前导零。因此，您可能想要在您的标题标签中使用`_SCORE(0)_`代替`_HITS_`来帮助邮件在一些`email`客户端中恰当地排序。SpamAssassin 3没有为

SURBL来配置使用JP列表，因此80_MDaemon_scores.cf文件增加了一条规则来支持它。而且，因为SURBL默认分值比MDaemon原先使用的要低，老的分值被放置在80_MDaemon_scores.cf文件中。根据您的需要来调节这些分值或删除这些行来使用默认值。新的默认贝叶斯得分被添加到80_MDaemon_scores.cf文件中。将来，这个文件将永远包含贝叶斯规则的默认分值。您可能希望要从您的local.cf文件中删除不同的"score BAYES_xx"行来使用新的默认值。

· 您的AntiVirus升级进度文件(MDaemon\App\AVSchedule.dat)被更名为"...\AVSchedule.dat.old"，因此一个全新的默认更新时间集能被放置在恰当的位置。新的默认更新发生时间是随机的，并且每天安排一个单个的更新。这能通过防止全球范围内过多MDaemon服务器在同一时间更新，因此可以提高更新速度。如果您宁愿使用您原先的设置，那么您可以通过重命名"...\AVSchedule.dat.old" to "...\AVSchedule.dat"文件来恢复您先前的AntiVirus更新进度。

· 请注意原先的MDaemon GroupWare产品已经更新发展成全新的Outlook Connector for MDaemon。这个名称的改变反映在MDaemon软件内部以及相关文档的众多方面。
要获知更多有关这项改变的信息，请参见如下文档：
http://files.altn.com/static/images/partners/press/newsletters/NL-200501.pdf

· 默认的自动垃圾邮件过滤IMAP规则已经改变。这个规则是为每个账号创建的，通过选中位于垃圾邮件过滤器的垃圾邮件过滤标签中(点击安全>垃圾邮件过滤器...)的*"自动过滤垃圾邮件到用户的IMAP垃圾邮件文件夹中"* 选项。这个规则仅用于检查每个邮件标题中是否存在X-Spam-Flag。这是不够的，因为一些外部的SpamAssassin的软件在邮件中放置"X-Spam-Flag: No"。 因此这个规则被改变成检查"X-Spam-Flag: Yes"而不是仅在标题中存在。要对您所有的账号改变此规则，清除*"自动过滤垃圾邮件到用户的IMAP垃圾邮件文件夹中"* 选项，并完成接下来的指令。这将从每个账号中移除旧的规则。然后，只要再点击复选框来为每个帐号创建新的规则。

· 如果您正在主界面中使用集成日志窗口，请在设置－>其它选项>GUI检查您的设置。它们可能需要调整，因为已经为激活Outlook Connector添加了新的日志，这可能会改变您先前的设置。

· 老版本的ComAgent不再与MDaemon8同步联系人。要重新获得这个能力，您的用户必须升级到ComAgent 8。

· 参见Relnotes.txt文件，它位于MDaemon的\Docs\子目录中。它包含了MDaemon从上个版本升级到该版本包含的所有新功能特性，改变和修正的列表。

安装

MDaemon Server v8 需要 Microsoft Windows 9x/NT4/2000/XP 或者更好的计算机系统，与 Pentium III 500MHz 等同的微型处理器，以及 256MB 内存或更多（推荐计算机 1GHz CPU 和 1GB 内存）。SMTP/POP/IMAP 及相关服务需要 Winsock TCP/IP 堆栈，就像 Microsoft Windows 所附带的，以及一个有 ISP 提供的互联网访问。如果您仅把 MDaemon 当作一个内部邮件服务器（您不使用它发送和接收外部邮件），那么 ISP 则不是必须的了。

安装 **MDaemon Server v8，点击开始 ⟶运行…** 然后输入在您的 MDaemon 安装包中提供的安装可执行文件的路径，然后点击“确定”。另外，您也可以通过使用控制面板中的“添加/删除程序”来安装 MDaemon。

安装程序将会提示您一些基本信息，例如注册名以及 MDaemon 文件所在的根目录。安装过程也提供逐步配置向导，它可以引导您进行最常用的设置。

参看：

主域设置—36页
新帐号的默认值—289页

也请参看：

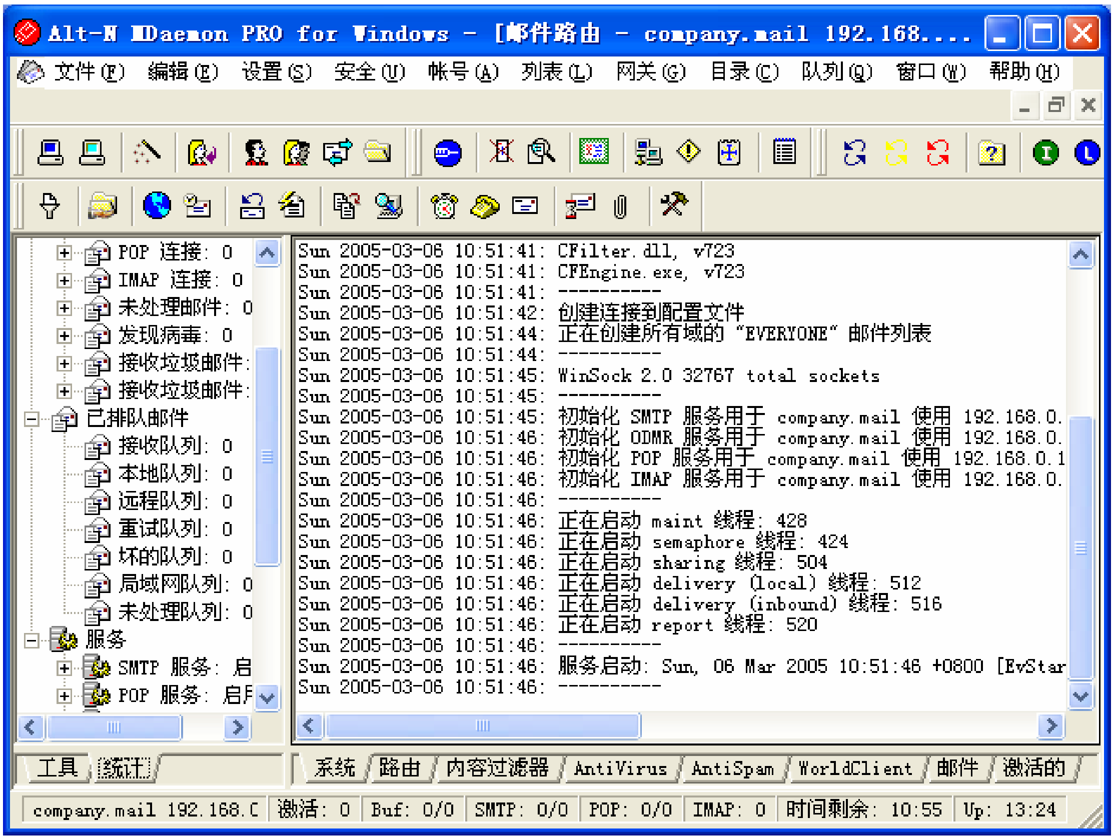
DomainPOP 邮件收集—212页

第二章

MDaemon ® 中文版

MDaemon的主界面

MDaemon 的主图型用户界面（GUI）在每次程序启动时自动启动，并给您有关 MDaemon 资源、统计、活动会话、和等待被处理的队列中的邮件的重要信息。也包括方便激活或者关闭 MDaemon 各种不同服务器的控制。GUI 的标签面板可以保持最新的状态来查看服务及输入输出连接的运行情况等等。



统计和工具

MDaemon 主界面左侧的默认面板包括两个标签：工具和统计。工具标签包括一个主域和每一个次域条目。在每一个条目下有一个对应不同对话框的快捷图标，被用来配置域和用户。统计标签包括3个部分：统计、队列邮件和服务。右键点击这一部分上的任何控件都会打开一个与操作相关的快捷菜单。

统计部分包括MDaemon 收发的邮件数量的统计以及从启动开始，初始化的邮件会话的数量的统计。这个部分会告诉您有多少用户已经使用，以及还有多少能被创建。统计包括 2 个右键快捷菜单：一个是用于账户控制，一个是用于统

计控制。账户快捷菜单提供快捷方式来创建、编辑以及删除账户。面板的剩余部分有一个快捷菜单，可以被用来清除列在下一个给出的控制上的计数。

队列邮件部分包括一个对每个邮件队列的条目和每一个队列包含邮件数量。可以右击每个队列打开快捷菜单来处理队列并打开队列管理器，通常用来查看、复制、或者删除队列的内容，就像其他功能一样。

服务部分包括了一个对 MDaemon 内每一个服务的条目，而且每一个条目都列出了服务的当前状态：“活动”或者“不活动的”。如果服务当前为活动的，以下所列的各个条目都是服务正在监听的端口。快捷菜单提供了在每一个服务的活动和非活动状态间切换的控制。

消息与事件跟踪

默认的主界面的右手侧包括几个标签。它们显示出 MDaemon 的各种服务和资源的状态，并且经常更新以反映当前的服务状况。

MDaemon 的 GUI 的主栏里面包括以下标签：

系统 - 在程序启动时，系统标签会显示一个*初始化过程*的日志，它可以提醒您 MDaemon 配置或者状态的可能存在的问题。也会显示例如 MDaemon 不同的服务激活/禁用的活动。

路由 - 为每一个通过 Mdaemon 处理的邮件显示路由信息。（发送到、来自于、邮件 ID 等等）

内容过滤器 - MDaemon 内容过滤器处理程序被放在此标签上。当一条信息符合内容过滤器的邮件规则标准之一时，这封邮件的相关信息以及操作都回被记录下来。

AntiVirus - 如果您安装了 Mdaemon AntiVirus，所有的反病毒处理都会被列到此标签上。当一个邮件被检查出了病毒，这封邮件的相关信息以及操作都会被记录下来。

AntiSpam - 显示所有的 MDaemon 垃圾邮件过滤器和阻拦活动。

WorldClient - 显示 WorldClient 的进程活动。

邮件 - 点击这一标签则其他几个邮件相关标签将会在此格中出现。

- **SMTP(in)** - 所有使用 SMTP 协议的进入的会话活动都会在此标签上显示。
- **SMTP(out)** - 所有使用 SMTP 协议的出去的会话活动都会在此标签上显示。
- **POP** - 当用户从 MDaemon 使用 POP3 协议接收邮件时，此活动会被记录。
- **IMAP** - 使用 IMAP 协议的邮件进程会被记录在此标签。
- **MultiPOP** - 此标签显示 MDaemon 的 MultiPOP 邮件收集活动。
- **DomainPOP** - 此标签显示 MDaemon 的 DomainPOP 活动。
- **LDAP** - 显示 LDaemon 的 LDAP 活动。
- **RAW** - RAW 或者系统生成的邮件活动被记录在此标签上。

激活的 - 点击此标签，其他几个标签将会显示在此格中。这些标签显示连接到 MDaemon 每个活动条目。无论连接的是出或入的 SMTP、POP、IMAP、WorldClient 或者其他类型，每一个激活的进程的信息都会在这里显示。

注意
在这些标签上面的信息不会对事实上存储在日志文件中的数据量有任何影响。然而，MDaemon 对关于记录文件中的信息类型和数量具有很强的适应性。更多的日志选项信息，请参看日志文件对话框（249 页）

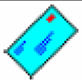
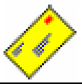
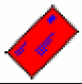
组合日志查看

组合日志查看选项位于 MDaemon 菜单栏中的窗口菜单。点击此选项将会添加一个窗口到主界面,这个窗口将会把 1 个或者多个标签上的信息组合并显示在一起。在杂项选项上的对话框 GUI 标签(259 页)上可以控制指定哪一个标签的信息会被组合到此窗口中去。

注意
在邮件路由窗口中的样式并不局限于以上所描述的默认位置。您可以通过选择窗口菜单选项来改变布局，然后点击切换窗格来控制希望切换到的布局。

托盘图标

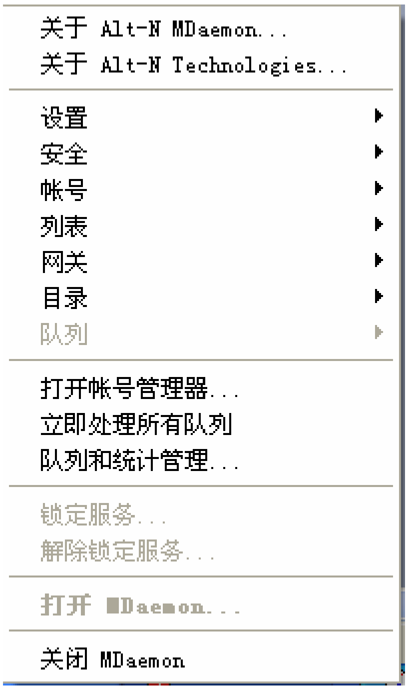
无论 MDaemon 服务器何时运行，它的图标都会显示于系统托盘中。然而，除了让您方便的知道服务是否运行以外，图标也是动态的并根据当前服务器状态更改颜色。下面是图标指示的列表：

	全部正常。在本地或远程队列中没有邮件。
	全部正常。在本地或远程队列中有邮件。
	磁盘允许空间低于临界值。（参看 271 页）
	网络断开、拨号失败、或磁盘空间已满。
图标闪烁	MDaemon 已经有新版本

关于服务器的附加信息会通过图标的工具提示显示出来。将鼠标指针放到图标上面，系统提示就会出现。

系统提示的第一位信息显示的是主域名称。下一个是它的 IP 地址。最后，字母“Q”（表示邮件队列），之后的数字是表示队列中邮件数量的2个数字。第一个数字指出在远程队列中的邮件数量。第二个数字指示的是本队队列中的邮件数量。

快捷菜单



在MDaemon托盘图标上点击右键打开快捷菜单。此菜单让你能快速访问所有 MDaemon 菜单和功能，而不用打开主用户界面。

点击在快捷菜单顶端部分的“关于 Alt-N”选项，可以找到更多关于 MDaemon 或者 Alt-N Technologies的信息。

在第二部分，你可以进入以下 MDaemon 菜单：设置、安全、账号、列表、网关、目录、以及队列。这些层叠菜单中的每一个和主界面菜单栏上面有相同名字的项目。

第三个部分打开帐号管理器和队列及统计管理器，而且其中的一个会让所有的 MDaemon 邮件队列被处理。

接下来，是控制锁定或者解锁 MDaemon 界面和关闭 MDaemon 的项目。

锁定/解锁 MDaemon 主界面

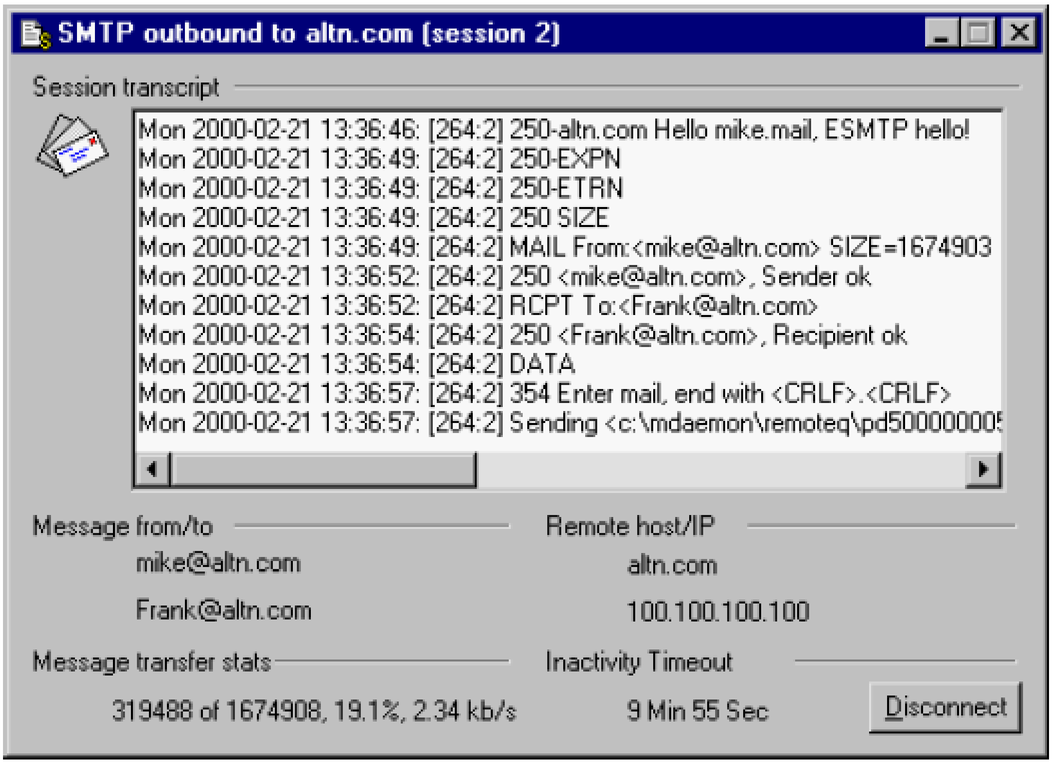
锁定用户界面，最小化 MDaemon，点击“锁定服务…”，之后在打开的对话框中输入一个密码。等待几秒，在确认密码之后，MDaemon 的用户界面将会

被锁定；它无法被打开或者被查看，尽管 MDaemon 还是会正常的继续运行功能。但是，如果您需要的话，您可以继续使用在此菜单上的"立即处理所有队列…"功能来手动处理邮件队列。解锁 MDaemon，双击托盘图标或者右击图标，选择"打开 MDaemon…"或者"解除锁定服务…"，然后输入您锁定时候时创建的密码。

最后，通过点击"打开 MDaemon…"菜单部分，您可以打开 MDaemon 服务界面。

连接窗口

当服务器检测某些远程客户端到请求，或者任何时候服务器初始化一个会话收集或者发送邮件时，每次都会出现一个连接窗口。此窗口将会通知您处理状态，以及警告您在邮件进程会话中遇到的任何问题。



进程传送脚本

此窗口显示所有的 i/o 会话。

远程主机/IP

此窗口告诉您MDaemon 和与之交互的远程计算机的名字及 IP 地址。

邮件来自/发到

此窗口显示发送者的地址和回信的地址。

邮件传送统计

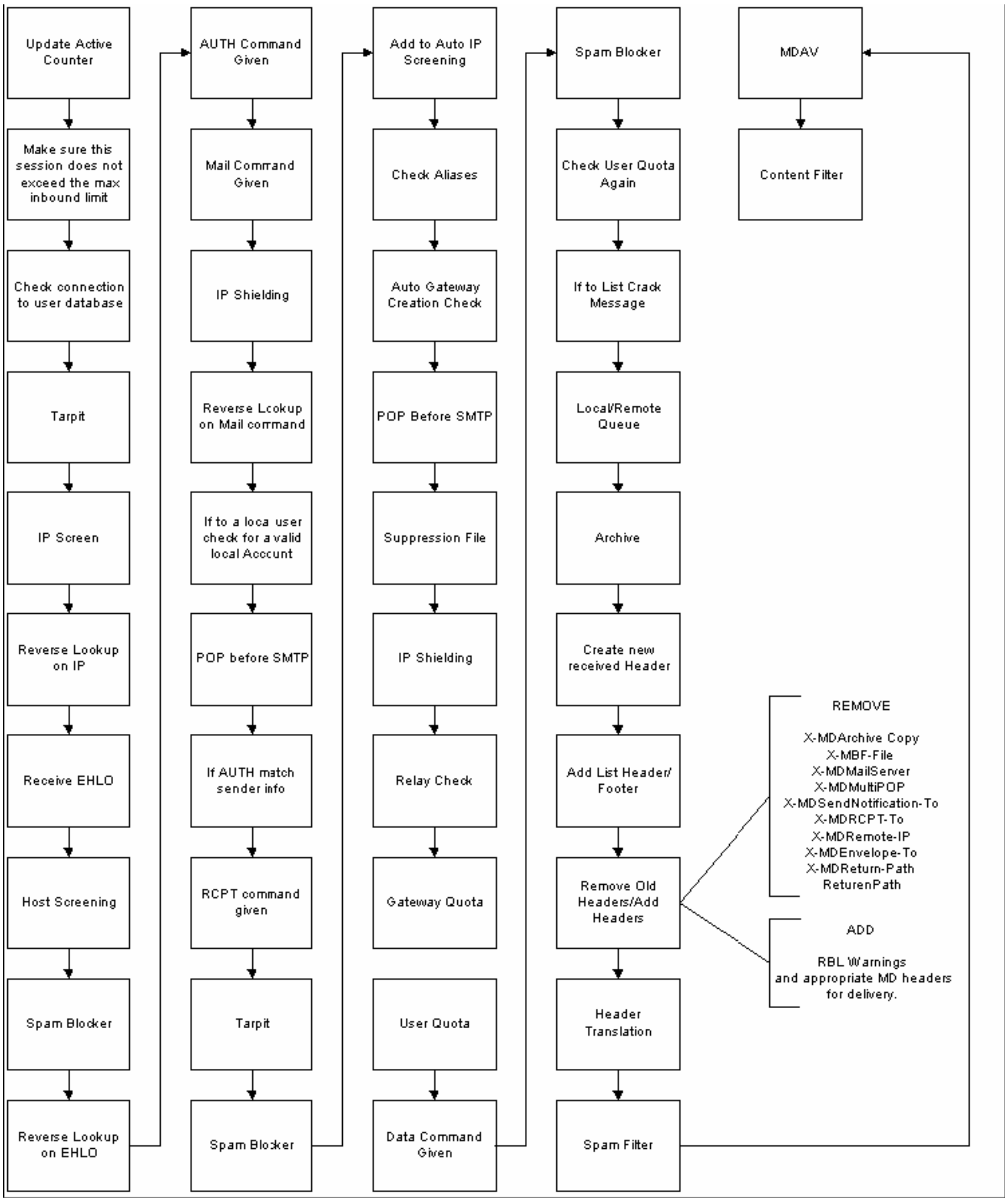
这里记录的是从远程系统中传送过或者收集到的字节数量的一个实时统计，是完全的百分比，和当前传送的速度。

不活动的超时
此计数器显示在 MDaemon 关闭会话前还剩下多长时间。

断开
此按钮会立即从远程系统断开服务。

MDaemon 的 SMTP 工作流程

当一个进入的 SMTP 连接创建时，MDaemon 通过一系列复杂的处理步骤来检查是否接受投递的邮件，而且如果一旦接受就继续做下去。下面的图标是对内部 SMTP 信息工作流程的图形化的表述。**注意：**哪些步骤被执行依赖于您的配置。如果在您的配置中一个功能被关闭的话，那么一个或者多个步骤将会被跳过。



第三章

MDaemon ® 中文版

MDaemon 的主域配置

域配置编辑器

域配置编辑器可以通过**设置 – 主域…**菜单进入，并且允许您设置几个您的域设置信息的关键部分中。您的主域是默认域名和一套您的用户用来收发他们的邮件的配置选项。一旦设置了一个主域，那么 MDaemon 就可以为任意数量的次域管理邮件（只限于MDaemon专业版），以及储存任意数量的域网关。

请参看：

次域编辑器

域网关

域设置编辑器是一个包括以下部分的标签式的对话框，这一功能对配置MDaemon v8是非常重要的。

域

这个对话框包括了您的主域的名字和 IP 地址，还有您的 HELO 域名称和机器名。

发送

这里，这个对话中包括您的主域名和 IP 地址，以及您的 HELO 域名和机器名。

端口

在这个对话框中，可以指定让 MDaemon 监听并且为 SMTP 和 POP 邮件发送使用的端口。您也可以指定 MDaemon 监听IMAP事件的端口，和被用来询问 DNS 服务器的 UDP 端口。在大多数情况下，不需要对默认的设置作任何改动。然而，当您需要将 MDaemon 和其他产品在您的机器上结合使用时，设置这些端口设置是非常有用的。

DNS

此对话框被用来指定主要和备份的 DNS 服务器 IP 地址。同时也包含管理 MDaemon 的 MX 操作以及 A 记录和在邮件发送过程中所发生的 SMTP 错误的各种控制。

计时器

这个区域包括了各种不同的时间限制，这些限制被 MDaemon 用来观测连接远程主机，等待协议对话框，等待 DNS 服务器回应及其他等活动。另外，这个对话框也包含*最大信息跳计数*限制，这个功能可以被用来帮助阻止从发送循环中截

获的邮件。

线程
这里您可以指定 MDaemon 用于收发SMTP，POP和IMAP邮件同时进行的最大进程数。您也可以指定MDaemon试图*在同一时间内*收发邮件的信息数量。另外，如果您选择，您可以捆绑在每一个线程上发出的SMTP邮件的数量极限。

出列
使用出列标签可以使MDaemon自动的发送ETRN，QSND或者类似的命令到ISP上，以便于使MDaemon将您保存的邮件出列，这样做您就可以通过SMTP收到这类的邮件而不是DomainPOP了。

存档
使用档案标签，可以保存由MDaemon处理的进出邮件的副本。您也可以选择是否让这份档案包含邮件列表或者MultiPOP信息或者忽略。

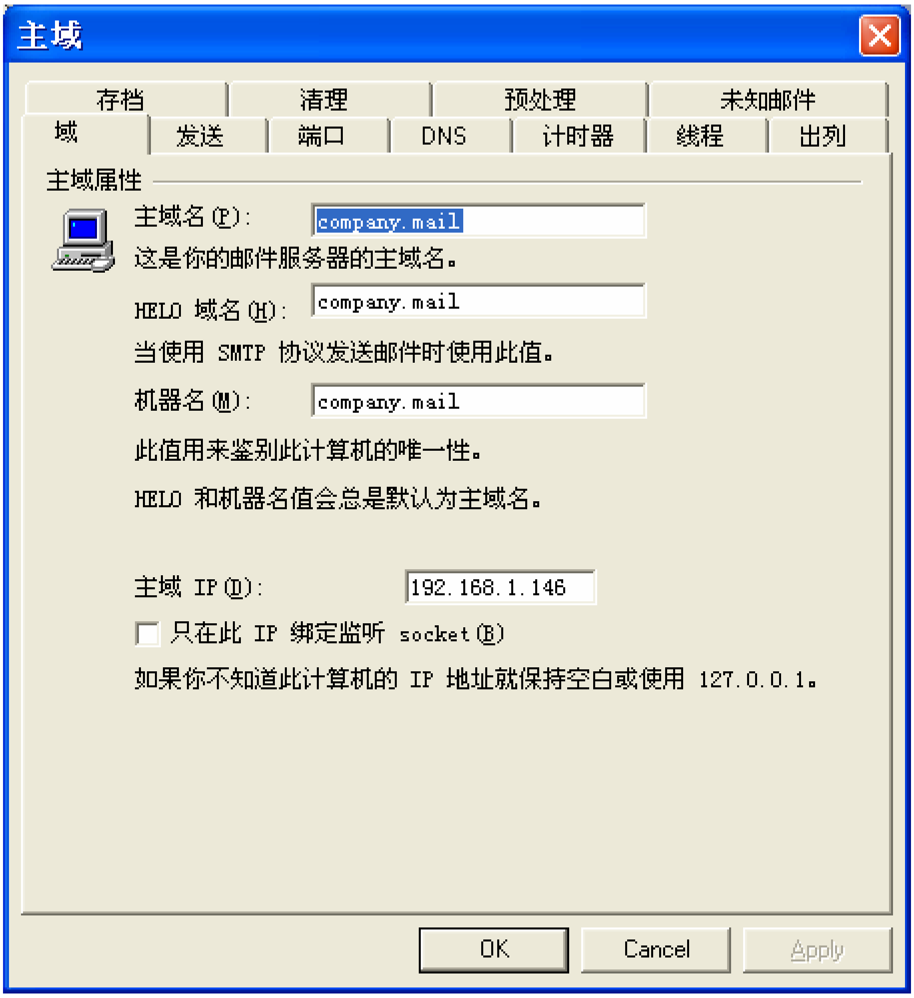
修剪
这个标签用来表示不活动的邮件在其被删除前可保留的时间。也包括对限制可被存储的信息的长度的控制。

预处理
这个对话框用来指定任何您希望在处理和收发邮件前，MDaemon立即运行的程序的路径。您也可以设置MDaemon在相关操作时的参数。

未知邮件
当一个来自本地域内的邮件地址的，却不是已知或者定义的用户的邮箱的邮件时，这个对话框里面包括的各种选项将使您控制MDaemon如何去做。各种不同的控制选项包括：发送邮件信息返回到发送者，发送邮件到邮递管理员，将消息放到坏消息队列，以及转发此消息到其他主机。这些控制都可以单独或者以各种组合的形式设置

请参看：
创建多个域的主机-64页
域网关-376页
也可以参看：
DomainPOP邮件收集-212页

域



主域属性

主域名

在这里输入您的主域名。当创建新帐号的时候，会使用默认的域名。很具代表性的，这里输入的值将是已经被注册过为网络域名并且可以让DNS服务器解析到本地运行服务器的IP地址或者此名称的一个有资格的别名。

作为选择，在某些情况下，您也可以选择一个虚构的域名称给您的主域名称（例如“company.mail”）。在这种方式下设置您的服务器，使用**邮件头翻译**功能（190页），和/或**域名称替换引擎**（216页）来授权合理邮件的发布是非常必要的。

HELO域名

在发送邮件时，这个域名称将会被应用到SMTP HELO/EHLO指令中。在大多数情况下，这将会是您的主域名称。

机器名

这个名字将会插入到邮件接受邮件头中。当您在一个主域中使用超过一台机器（例如做一个备份服务器），通过系统和在邮件头中单一IP地址和域名称来追踪邮件路径是一件非常困难的事情—而知道是哪一台机器处理这个邮件是更为困

难的。邮件头中插入一个名字可以使明确的区分每一个处理邮件的机器这个工作变简单。如果您在这个控制中，不能提供明确的区分器，那么主域名称还会被使用。

主域IP

这个是主域的IP地址。

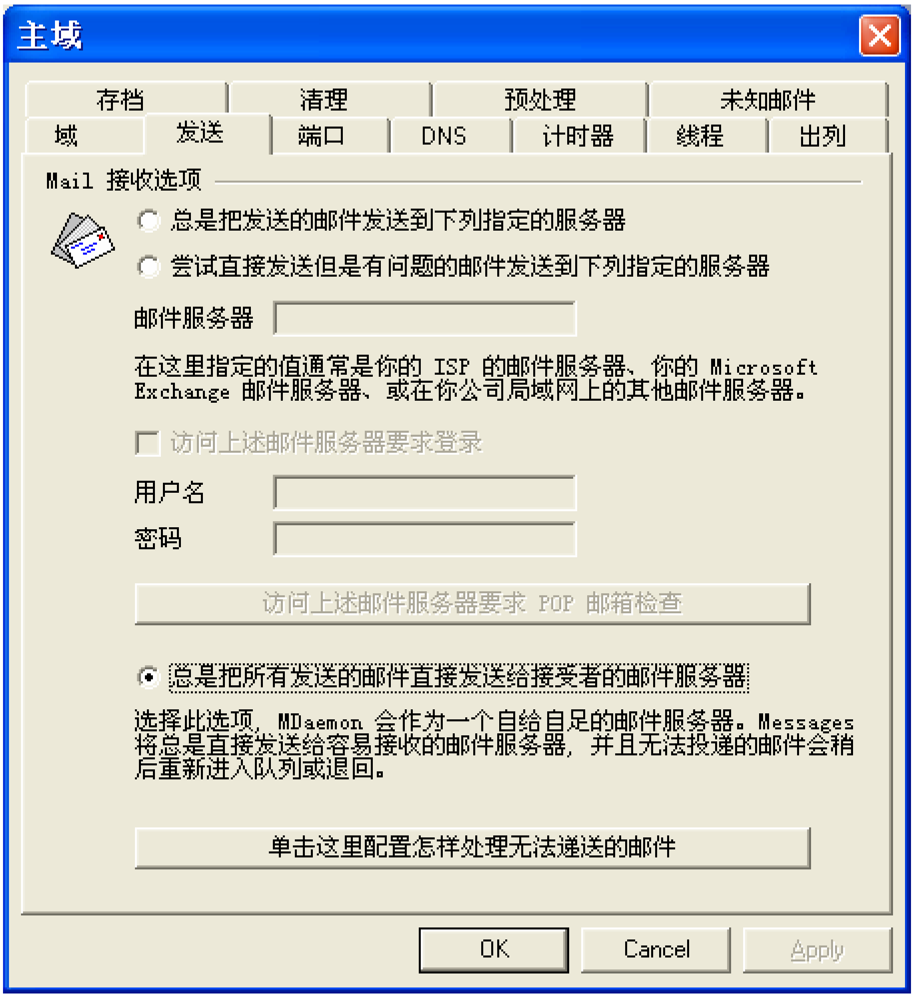
只在此IP绑定监听 socket

选择这个开关，可以使得MDaemon使用在域IP文本框中找到的特定IP地址并绑定它的网络端口。通常在创建多个域的时候，这个控制需要在某些特定环境中使用

此类设置的更多信息，请参看

创建多个域的主机-64页

发送



邮件传递选项

总是把发送的邮件发送到下列指定服务器

如果您想让所有的外发邮件，无论是不是在它的目标域，都为投递到一个网关主机，请选择此选项。如果选择了，那么所有的外发邮件都将发送到文本框中指定的ISP*或者主机IP或域名*发送。很显然，这一功能在直接邮件投递造成服务器资源额外压力的高流量期间是非常有用的。

尝试直接发送但是有问题的邮件发送到下列指定的服务器

如果您只想将未能投递的外发邮件发送到文本框中指定的ISP*或者主机IP或域名*，那么请点击此选项。无法发送的邮件是由于目的地址的邮件主机无法被解析到一个真实IP（比如到远程网络未注册的网关）或者发送的邮件虽被主机正确的处理，但却不能直接连接或拒绝直接连接造成的。这个选项将会使MDaemon将消息传递到一个更有力的MTA中，而不是将这些邮件返回到始发者。在您的本地服务器不能直接连接时，有时会通过您的ISP运行的邮件系统可能用路由的发式发送邮件。

邮件服务器

在这里，制定您的ISP或者邮件主机域名或IP地址。通常在您的ISP上的是SMTP

服务器。

注意
不要输入 MDaemon 的主域名称或者 IP 地址到这个文本框中。这里应该输入一个 ISP 或其他能够为您转发邮件的邮件服务器。

访问上述邮件服务器要求登陆
作为一种附加的安全方案，一些ISP需要他们的用户在通过服务器发送邮件前先登陆。如果您的ISP或者邮件主机需要此要求，那么请使用这个选项来指定您的登陆认证。

用户名
输入您的ISP用户名或登录。

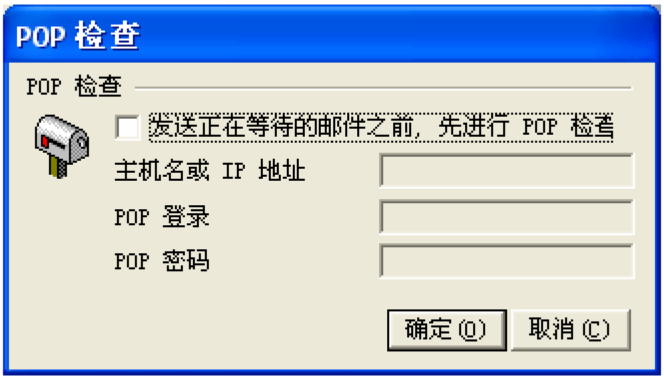
密码
使用这个选项指定您的ISP或者邮件主机的登录密码。

*访问上述邮件服务器要求**POP**邮箱检查*
作为一个附加的安全方案，某些ISP需要他们的客户在通过ISP服务器发送邮件前先登陆到一个POP邮箱。如果您的ISP或者邮件主机需要，请点击这个按钮，以打开POP检查对话框。

总是把所有发送的邮件直接发送给接受者的邮件服务器
当这个选项被选中时，MDaemon将会尝试直接发送所有邮件而不是将邮件转发到其他主机上。MDaemon将会把为发送邮件放到它的重试系统中，通过您在重试配置对话框中设置的参数和时间间隔，继续尝试发送。您可以通过点击*单击这里配置怎样处理无法递送的邮件*按钮来访问这个对话框。

单击这里配置怎样处理无法递送的邮件
在发送过程中遇到问题时，您可以点击此按钮，以打开重试配置对话框，这样您就可以指定MDaemon多久将尝试发送此邮件。您也可以在尝试停止之后指定时间间隔，以及在最后一次尝试完成后对这些邮件做什么。请参看下面的重试配置对话框。

POP检查



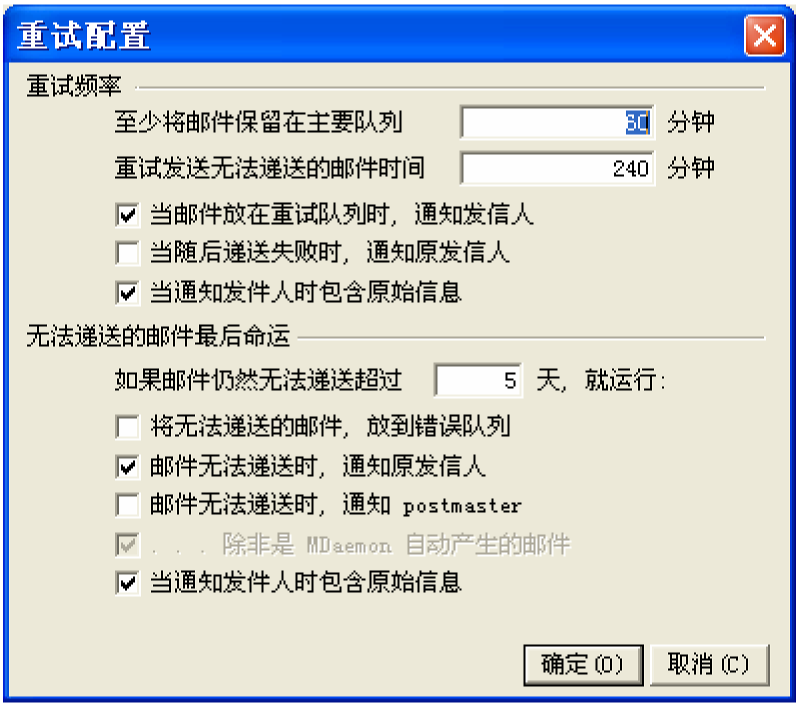
访问上述邮件服务器要求POP邮箱检查
如果您需要在发送邮件前执行POP检查，点击这个检查框。

主机名或IP地址
输入您希望的连接到主机或者IP地址。

POP登陆
这里是POP帐号登录或者用户名。

POP密码
这里是帐号的POP密码。

重试配置



重试频率

至少将邮件保留在主要队列 xx 分钟

这个设置控制邮件放到重试队列之前在主队列中保持的时间长短。主队列和重试队列相比，通常会更快更频繁的进行尝试。

重试发送无法递送的邮件时间 xx 分钟

这个设置决定了在重试队列中消息多久会被处理一次。

当邮件放在重试队列时，通知发信人

当发送人的邮件被放入重试队列中的时候，这个开关将提醒他/她。这个消息的文本内容可以在 DELWARN.DAT 中找到（或修改）。

当随后递送失败时，通知原发信人

如果投递尝试在重试队列中的一封邮件失败了，那么一封解释此事件的消息会被发到这个邮件的发件人那里。这个消息的文本内容可以在 DELWARN.DAT 中找到（或修改）。

当通知发件人时包含原始信息

点击此选项，可以将原邮件作为一个附件包含在以上的提示信息中发送给发件人。

无法递送的邮件最后命运

如果邮件仍然无法递送超过 xx 天，然后：

这个设置决定了一份邮件在移除前可以保留在重试对列中的天数。

将无法递送的邮件，放到坏队列

当这个选项被钩选后，一旦有一封邮件达到了*如果邮件仍然无法递送超过 xx 天，然后：*选项所设置的期限时，就将该邮件的移动到坏邮件目录下。

邮件无法递送时，通知原发信人

当这个选项被钩选后，一旦有一封邮件达到了*如果邮件仍然无法递送超过 xx 天，然后：*选项所设置的期限时，MDaemon 就会发一条信息通知发信人该邮件已从服务器中永久删除。这个消息的文本内容可以在 DELWARN.DAT 中找到（或修改）。

邮件无法递送时，通知 ***postmaster***

当这个选项被钩选后，当邮件信息从重试系统中永久删除后，会通报postmaster。

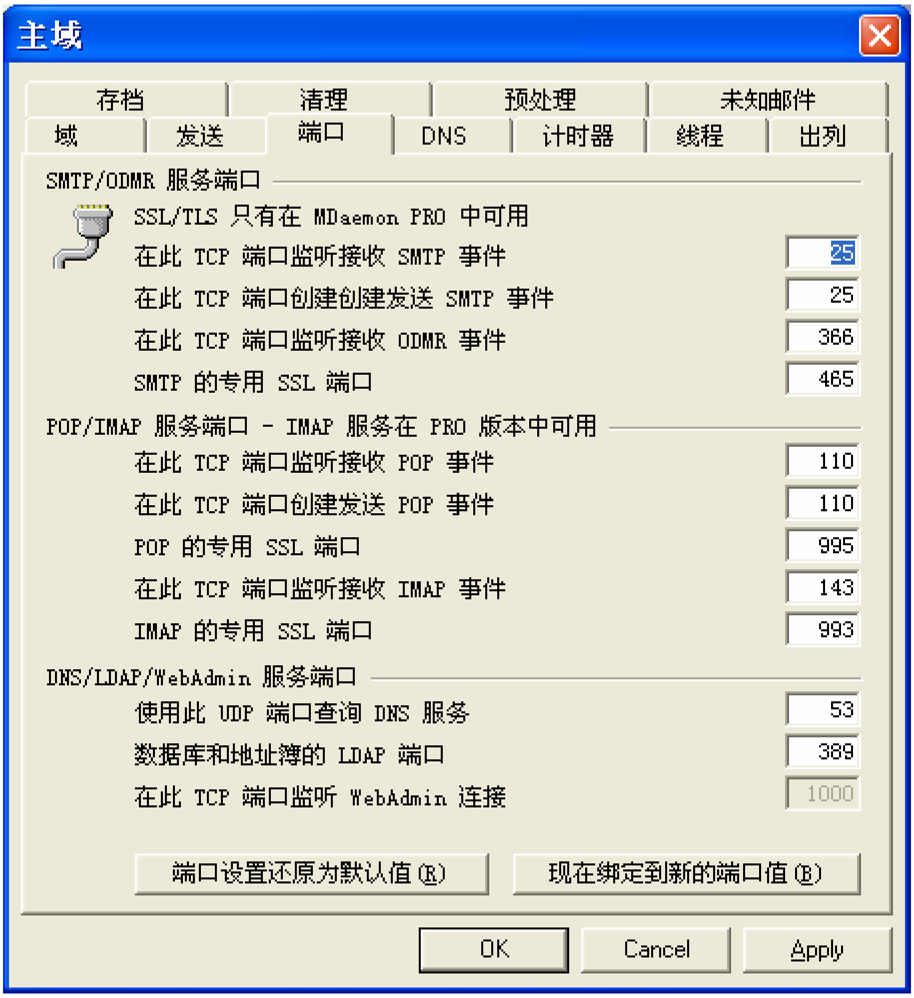
***…**除非是**MDaemon**自动产生的邮件*

当自动生成的邮件递送失败时，重试系统不会通知到MDaemon。然而，因为这种信息可能对postmaster很有用，所以当这些邮件无法递送时就会通知到他/她。如果当自动生成的邮件无法递送时，您不希望通知postmaster的话，就点选此项。自动生成邮件是指回执通告，生成自动回复邮件，帐号结果处理等。

<u>当通知发件人时包含原始信息</u>

在发送邮件递送失败信息给发件人时，点击此选项可以将原始邮件作为附件一起发送。

端口



SMTP/ODMR服务端口

<u>在此TCP端口监听接收SMTP事件</u>
MDaemon将会在此公司监听从SMTP客户端连入的连接。

<u>在此TCP端口创建发送SMTP事件</u>
当发送邮件到其他SMTP服务器时，将使用此端口。

<u>在此TCP端口监听接收ODMR事件</u>
MDaemon会在这个端口上监视进入的ODMR连接，例如来自域网关的ATRN。

<u>SMTP的专用SSL端口</u>
这个端口是使用SSL连接专门进行SMTP邮件通话的。更多信息，请参见SSL&证书-153页。

POP/IMAP服务端口（IMAP服务在PRO版中可用）

<u>在此TCP端口监听接收POP事件</u>

MDaemon会从在此端口监听远程POP客户端上连入的连接。

在此TCP端口创建发送POP事件
使用此端口，从POP3服务器上取得邮件。

POP的专用SSL端口
这个端口是使用SSL连接，专门为POP3邮件客户端所用。更多信息，请参见SSL&证书-153页。

在此TCP端口监听接收IMAP事件
MDaemon将会用此端口来监听进入的IMAP请求。

IMAP的专用SSL端口
这个端口是使用SSL连接，专门为IMAP邮件客户端所用。更多信息，请参见SSL&证书-153页。

DNS/LDAP/WebAdmin服务端口

使用此UDP端口查询DNS服务
输入您希望MDaemon用来收发数据报到DNS服务的端口。

数据库和地址薄的LDAP端口
MDaemon将会使用此端口发送数据库和地址薄信息到您的LDAP服务器。

请参看：LDAP地址薄支持 -109页

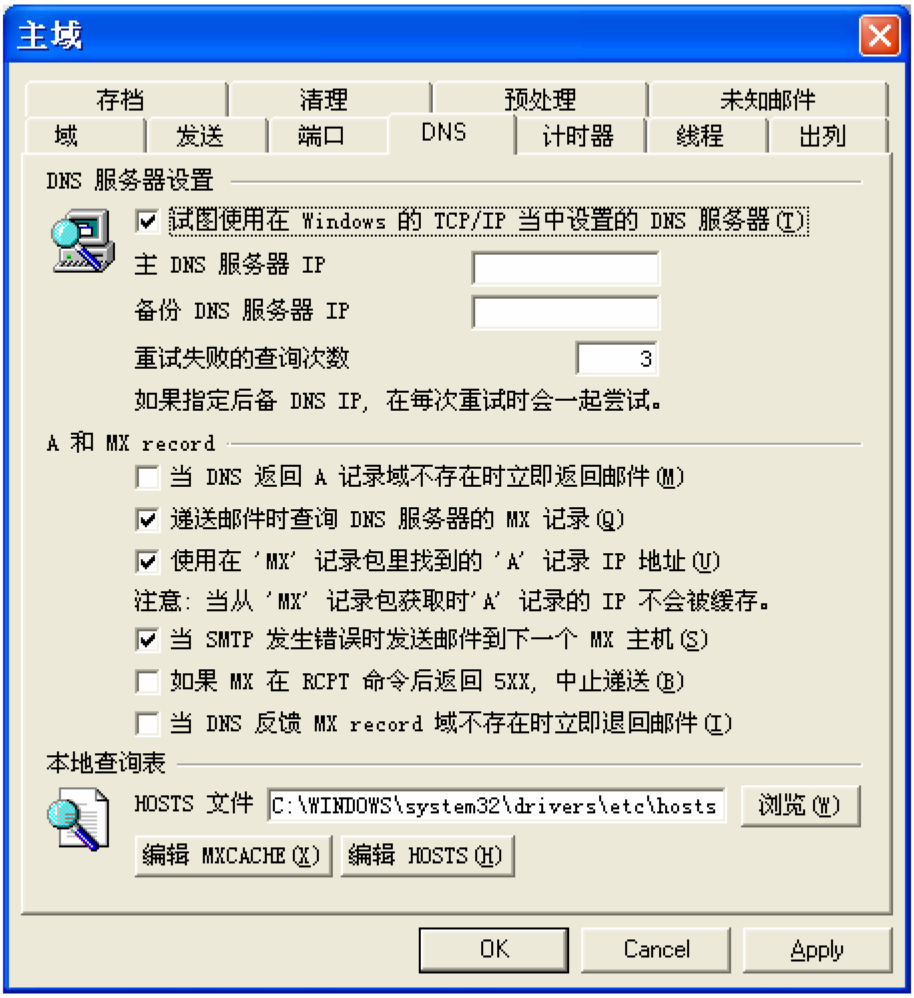
在此TCP端口监听WebAdmin连接
这个端口将会监听WebAdmin连接。

端口设置还原为默认值
这个按钮将会使端口设置变回它们的标准值。

现在绑定到新的端口值
当您对任意的端口值设置进行了改动时，您需要按此按钮使得您的更改能够立刻起效。否则，您的更改在下次服务器启动前，都不会被应用。

注意
上述的端口设置已经是对合适的服务器操作进行了鉴定的，除非您确定您确实需要，否则就不应该更改设置。设置 MDaemon 使用的端口可以允许使用代理系统或者其他需要某些端口号的软件服务进行操作。 一个 IP 地址（一台机器）只能有一个可用的端口。如果其他程序试图连接已经在被另一个程序所使用的端口，那么一个错误信息将会提示使用者所需地址（IP：PORT）正在使用中。

DNS



DNS服务器设置

试图使用在windows的 TCP/IP当中设置的DNS服务器

Windows在本地TCP/IP配置中，有时会保持一个DNS服务器IP地址。如果这种情况发生在您的电脑上，您要检查此设置。如果MDaemon不能找到本地持有的DNS服务器，那么它将会使用这个屏幕中指定的。

主DNS服务器IP

输入您希望MDaemon询问‘A’和‘MX’记录的DNS服务器的IP地址。为了确保合理的操作，这个条目必须指定。

备份DNS服务器IP

输入您希望MDaemon询问‘A’和‘MX’记录的备份或者次要DNS服务器的IP地址。此设置可选，但我们推荐您这么做。

重试失败的查询次数

如果一个查找尝试失败了，MDaemon将会重复查找设置中的次数。如果您制定了一个备份的DNS服务器，那么这两个服务器都将包括查找尝试。

MX Record处理

当DNS返回A记录域不存在时立即返回邮件

点击此选项，在DNS查找显示A记录域不存在时，可使MDaemon立即退回邮件。

递送邮件时查询DNS服务器的MX记录

如果您希望MDaemon在尝试发送邮件时，询问您指定的DNS服务器查找‘MX’，那么请启动此功能。

使用在‘MX’记录包里找到的‘A’记录IP地址

如果您希望MDaemon尝试到‘A’记录IP地址的投递（在这些在‘MX’记录处理过程中被发现），那么请点击此检查框。

当SMTP发生错误时发送邮件到下一个MX主机

当这个功能激活时，MDaemon将继续尝试邮件投递到下一个MX主机，即使当前的‘MX’反馈了一个致命SMTP错误。

如果MX在RCPT命令后返回5xx，终止递送

通常情况下，在一个SMTP通话期间，当MDaemon受到了对RCPT命令的5xx回应，那么它就会继续尝试发送邮件到每一个MX主机。如果您想让MDaemon在收到这个反应时，放弃投递尝试，那么点击此检查框。

当DNS反馈MX record域不存在时立刻退回邮件

如果DNS查找反馈“域不存在”信息，点击这里，可以使MDaemon立即返回邮件。此功能会阻止这类邮件到重试这个循环。

本地查询表

HOSTS文件

在询问DNS服务器之前，MDaemon会首先通过Windows HOSTS文件来尝试解决一个地址。询问中如果该文件包含域IP地址，MDaemon将不再询问DNS服务器。

注意
您必须输入完整的路径和文件名而不仅是文件名。MDaemon 将会尝试使用以下值作为此文件的默认位置。 Windows 95/98 – [drive]：\windows\hosts Windows NT – [drive]:\windows\system32\drivers\etc\hosts HOSTS 文件是包含域名称的 A-record 或者主要 IP 地址的 Windows 文件。MDaemon 也允许您在一个叫做 MXCACHE.DAT 的文件里面制定 MX-record IP 地址。这个文件可以在 MDaemon\APP\文件夹下找到。在一个文本编辑器中载入 MXCACHE.DAT 文件，之后在文件的顶端阅读注释，寻找更多信息。

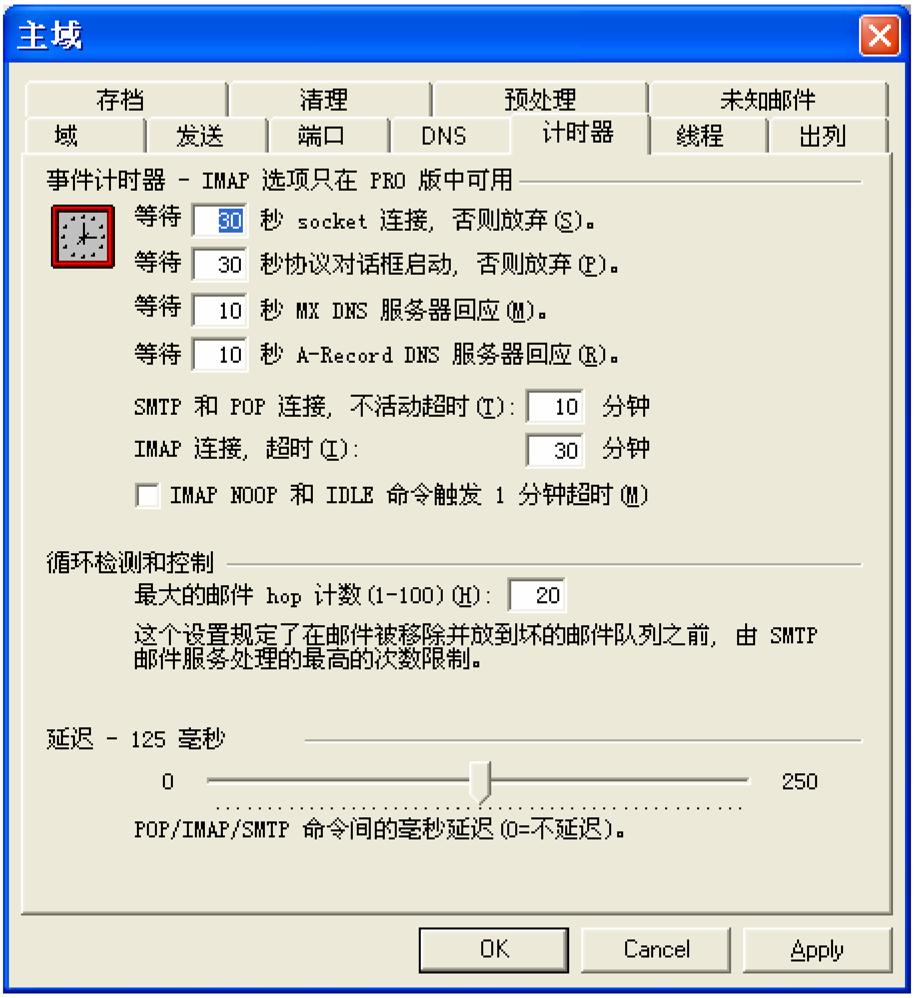
编辑 MXCACHE

点击此按钮使用 MDaemon 的文本编辑器察看或者编辑 MXCACHE.DAT 文件。

编辑 HOSTS

点击此按钮使用 MDaemon 的文本编辑器察看或者编写 HOSTS 文件。

计时器



事件计数器（**IMAP** 选项只在 **PRO** 版中可用）

等待 XX 秒 socket 连接，否则放弃

在初始化一个连接请求后，MDaemon 将会为远程系统准许访问等待几秒钟。如果远程系统没有在时间框中设置的时间内回应，那么 MDaemon 将会发送邮件到另外的网关主机或者重试队列，这依赖于您是如何选择设置在域设置编辑器上的域/ISP 标签（38 页）上的。

等待 XX 秒协议对话框启动，否则放弃

一旦远程主机创建了一个连接，这里会使 MDaemon 在开始 SMTP 或 POP3 协议对话框前，等待远程主机 XX 秒。如果远程主机没有在时间框中设置的时间内开始协议通话，那么 MDaemon 将会发送邮件到另外的网关主机或者重试队列，这依赖于您是如何选择设置在域设置编辑器上的域/ISP 标签（38 页）上的。

等待 XX 秒 MX DNS 服务器回应

当使用 DNS 服务为远程域解决‘MX’主机时，MDaemon 会等待对‘MX’的

回应几秒。如果 DNS 服务器没有在时间框中设置的时间内回应，MDaemon 将会尝试发送邮件到远程主机的‘A’DNS 记录中的指定的 IP 地址。如果尝试失败，MDaemon 将会发送邮件到另外的网关主机或者重试队列，这依赖于您是如何选择设置在域设置编辑器上的域/ISP 标签（38 页）上的。

等待 XX 秒 A-record DNS 服务器回应
计时器控制在试图解析一个远程主机的IP地址时，MDaemon将会等待多长时间。如果尝试失败，MDaemon 将会发送邮件到另外的网关主机或者重试队列，这依赖于您是如何选择设置在域设置编辑器上的域/ISP 标签（38 页）上的。

SMTP 和 POP 连接，不活动超时：XX 分钟
如果一个成功的连接和处理通话已经持续不活动了一段时间（没有 I/O），MDaemon 将会放弃这个处理。MDaemon 将会在下次计划处理时间中，再次重试。

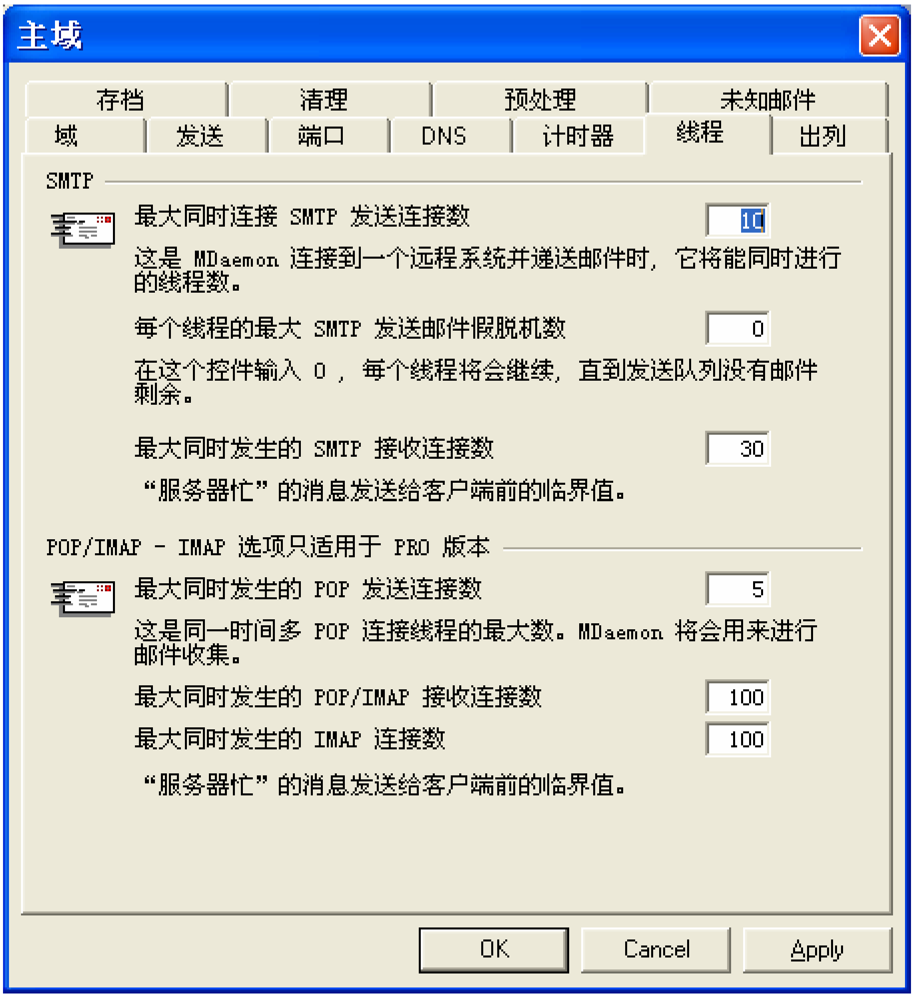
IMAP 连接，超时：XX 分钟
如果 IMAP 处于不活动状态中一段时间，那么 MDaemon 将会关闭这个连接。

IMAP NOOP 和 IDLE 命令触发 1 分钟不活动超时
当此检查框开启时，IMAP 不活动计数器会在遇到一个 NOOP 或者 IDLE 命令时，被设置成为一分钟。一些 IMAP 客户端会发布一些 NOOP 命令，以保持连接，即使已经没有了实际的邮件处理活动在进行。这个功能会阻止此类连接保留活动状态，以减少资源浪费，这一性能可以对更高容量的基于 IMAP 的邮件站点是极为有用的。

循环检测和控制
最大的邮件 hop 计数（1-100）
RFC标准规定邮件服务器在处理每一封邮件的时候都会都一个标记。这些标记会被记数并作为一种暂时的方法以解决由有时错误配置造成的邮件循环。通过记录被处理的邮件的次数，这些邮件可以被监测到并放入坏邮件目录中。假设如果在通过大量给定的邮件服务器跳数处理后，邮件还没有到达收件人，那么在进程里面就可能会有一个邮件循环。多半，此控制的默认设置因该足够去阻止邮件循环，而且不需要做任何改动。

延迟
延迟 – XX 毫秒
在 POP/SMTP/IMAP 协议命令之间，会有毫秒间隔。这对阻止处理信息快于收件人接受速度的高速连接是非常有用的。这个延迟只在 POP/SMTP/IMAP 协议命令序列才有效-即一个邮件信息文件的真实传送已经完全被缓冲-。

线程



SMTP

最大同时连接 STMP 发送连接数

这个数值将设置需要向远程系统发送邮件时，所能创建的最大远程 SMTP 线程数。每个线程都将发送远程邮件，直到任何队列中都没有邮件剩余，或者达到*每个线程的最大 SMTP 发送邮件数*所设置的值。例如，远程邮件队列中有 20 个邮件等待发送而且该设置的值为 5，那么将同时创建 5 个线程，而每个线程会连续地发送 4 个邮件。

您应该测试多少个线程对您的带宽来说具有最优异的性能。指定太多的对话可能导致您的带宽超负载或者您的 Windows 机器资源耗尽并且您将会失去投递的效率。请记得，每一个被 MDaemon 创建的 SMTP 线程都可以连续的投递邮件，因此，四个线程投递两个邮件要比八个线程各自投递信息执行的更快更好。一个好的启动应该是对 28.8K Modem 来说五到十个线程，对 ISDN 来说十到十五个线程。

每个线程的最大 SMTP 发送邮件数

这个设置对在线程停止发送邮件并从内存中释放自己之前，这些线程所发送的单独的邮件的数量做出了限制。通常的，您应该使这个控制设置为零，这样可使每一个现成连续发送邮件直到队列为空。

最大同时发生的 SMTP 接收连接数

这个值控制在服务器回应“服务器太忙”信息前，可接受同时发生的进入 SMTP 线程的数量。

POP/IMAP（IMAP 选项只适用于 PRO 版本）

最大同时发生的 POP 发送连接数

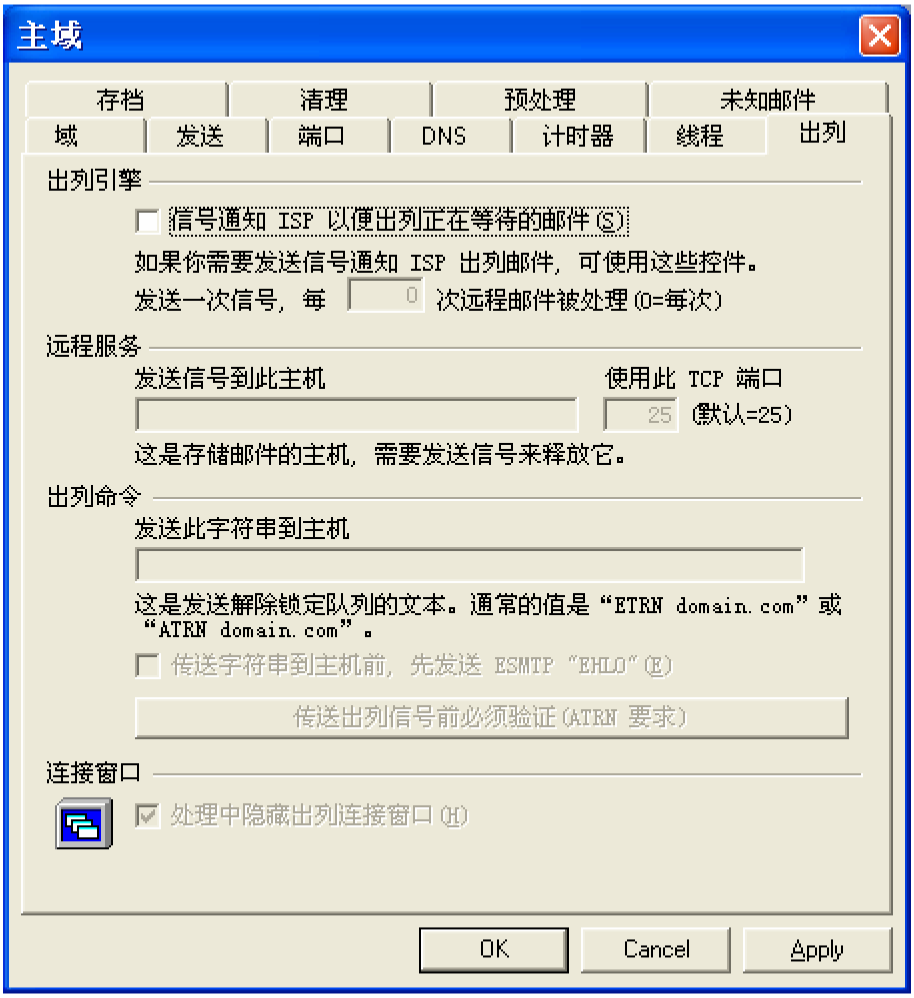
这里的值表示的是在收集 DomainPOP 和 MultiPOP 邮件时，被创建的最大可能出去 POP 连接数。每一个连接都将收集此类型的邮件，直到处理了所有的 DomainPOP 和 MultiPOP 服务器，并且收集到了所有的邮件。例如来说，如果在您的用户中有 15 个 MultiPOP 通话，这个值设置成三，那么之后每一个通话将会从五个 MultiPOP 资源中收集邮件。

您应该测试多少个通话对您的带宽来说具有最优异的性能。指定太多的对话可能导致您的带宽超负载或者您的 Windows 机器资源耗尽并且您将会失去投递的效率。请记得，每一个被 MDaemon 创建的 POP 通话都会收集邮件直到所有的资源耗尽。因此，四个通话从二十个资源里面收集邮件比二十个通话从一个单独的资源中收集要执行的更快更好。一个对启动好的地方，应该是对 28.8K Modem 来说五到十个线程，对 ISDN 来说十到十五个线程。

最大同时发生的 POP/IMAP 接收连接数

这个值控制了在服务器回应“服务器太忙”信息前，可接受的最大并发 POP 和 IMAP 进入邮件通话的数量。

出列



出列引擎

信号通知 ISP 以便出列正在等待的邮件

当处理远程邮件的时候，MDaemon 可以在任意端口上连接到任意服务器并且可以发送任何您想发送的字符串。当您需要通过发送一些字符串到服务器，来用信号通知远程服务器释放您的邮件，那么这是非常有用的。例如来说，ATRN，ETRN，或者 QSND。您也可以在暂时需要 FINGER 或者 TELNET 通话时，使用此功能，以便您的 ISP 检测您是否在线。

发送一次信号，每 xx 次远程邮件被处理（0=每次）

通过默认值，将每次都发送邮件已被处理的出列信号。输入数字到这个控制将会阻止出列信号每次都发送。通过制定的每 x 次发送。举个例子，设置这个值为 3 将会使远程邮件被处理的信号每 3 次发送。

远程服务器

发送信号到此主机

发送释放您的邮件的信号到您希望连接到的主机。

使用此 TCP 端口

输入您希望连接的端口。默认值为 25（SMTP 端口），适用于 ETRN 或者 QSND 信号方法。端口 366 是典型为 ATRN 使用的，端口 79 是为 FINGER 使用的。

出列命令

发送此字符串到主机

这个控制是为了指定需要发送的文本字符串的，以便于您的邮件可以被释放。例如来说，ETRN 方法需要在域名称后面跟着“ETRN”文本。其他方法需要发送其他的文本。如果您需要更多关于发送什么解锁您的邮件队列的信息，请查询您的 ISP。

注意：
当使用邮件主机的出列方法时，在允许的前提下，我们建议使用 On-Domain 邮件传递（ODMR）。我们相信对于在此方式下主机您的邮件，这是目前最好的方法。在此控制中，ODMR 需要使用 ATRN 命令。

传送字符串到主机前，先发送 SMTP“EHLO”

如果您开启这个复选框，您应该连接到一个 SMTP 服务器以发送释放您邮件的信号。这个开关使和一个指定的主机 SMTP 通话初始化，并且允许此对话在发送解锁字符串之前只进行到 SMTP“EHLO”阶段。

*传送出列信号前必须验证（**ATRN** 要求）*

作为一个安全方法，为了阻止未认证用户试图出列他们的客户的邮件，一些 ISP 要求他们的客户在发送出列信号前，通过 ESMTP AUTH 认证他们自己。如果您的 ISP 是这种情况，您可以通过点击此按钮，打开出列认证对话框。您可以在那里输入需要的认证信息。请看下面的出列认证。

注意：
当使用 ATRN 命令出列您的邮件时，认证是必须的。

连接窗口

出列中隐藏出列连接窗口

当在进行时，如果您想隐藏通话窗口，请点击此通话窗口

注意：
如果您在*发送信号到此主机*控制里面的值是域名称而不是一个 IP 地址，MDaemon 在试图解析此站点的 MX 记录，将会试图连接此站点的 MX 的 IP 地址。这是在假设您已经将 MX 引擎打开，并且正在工作（请参看 47 页 DNS）。如果输入的值是 IP 地址，不是域名称，之后将会使用那个 IP 地址创建连接。

On-Demand邮件传递（ODMR）

我们相信对于处理您的邮件，目前可行的最好的投递方法（队列/出列）是 On-Demand 邮件投递（ODMR）。因为在邮件出列前，需要认证，所以这个方法领先于 ETRN 和其他方法。而且，它利用被称作 ATRN 的 ESMTP 命令，这不再需要客户端（客户）有一个静态 IP，这是因为它可以快捷的倒转客户端和服务器端（提供者）之间的数据流，并且处理邮件不再使用创建新连接（和 ETRN

不一样）。
MDaemon 在客户端侧，通过使用在出列标签上的 ATRN 命令和认证控制，和在服务器端通过在网关编辑器上的 ATRN/AUTH 标签使用域网关，完全支持 ODMR（382 页）。
很多邮件服务器还不支持 ODMR，因此您应该在尝试前和您的服务商查询此事。

出列 AUTH*

出列验证

<u>当发送出列信息到主机，使用 ESMTP AUTH</u>

除了在发送邮件前，需要他们的客户认证他们自己外，许多 ISP 需要他们的客户在发送出列信号前，进行认证。如果需要您做这些，请点击此检查框，可以使 MDaemon 在尝试收集任何队列中邮件前，发送您的认证信息。

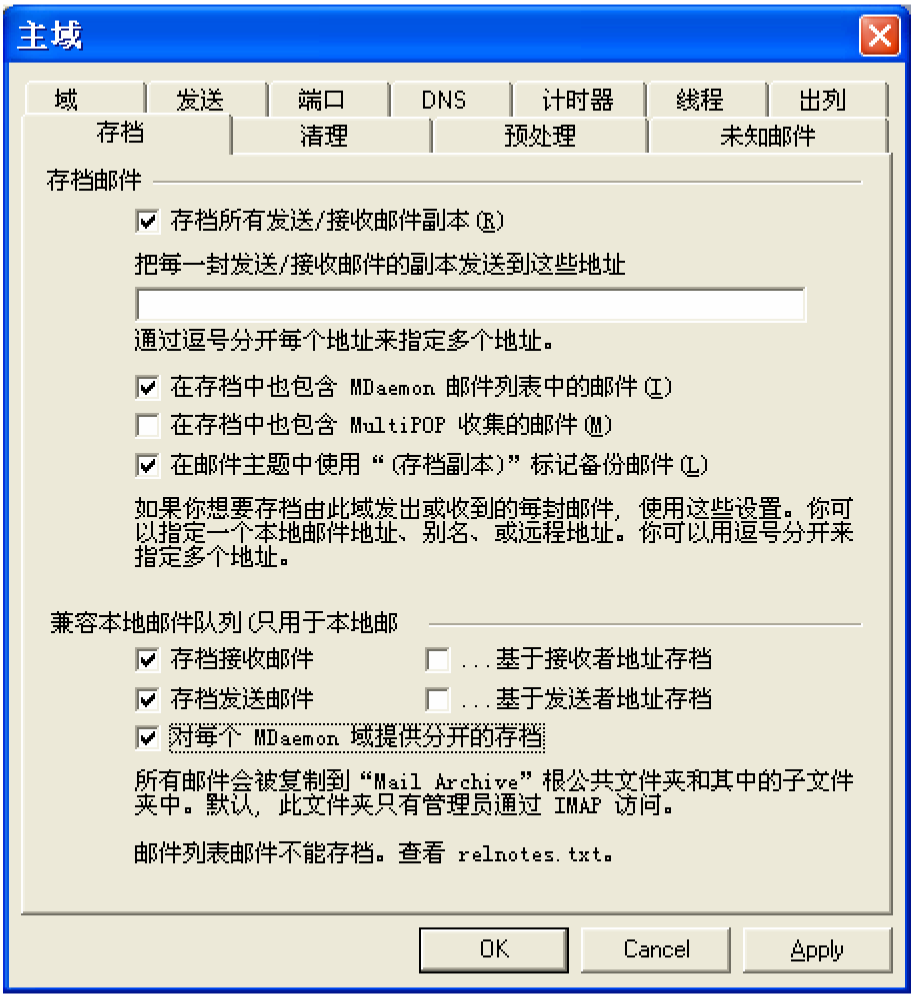
<u>AUTH 登录</u>

如果在发送出列您的邮件信号前，需要认证的话，那么请在这里设置需要的 AUTH 登陆参数。

<u>AUTH 共享密码</u>

请输入您的 ISP 要求的，在 AUTH 共享隐私中使用的密码。

存档



存档设置

存档所有发送/接收邮件副本

这个开关启动存档引擎。激活它将会使得所有通过服务器的进出邮件的一份拷贝发送到控制中指定的地址。

把每一封发送/接收邮件的副本发送到这些地址

输入一个或者多个您希望发送存档邮件的地址。多地址时需要用逗号隔开。您可以指定本地和远程地址以及地址别名。

*在存档中也包含 **MDaemon** 邮件列表中的邮件*

如果您想存档的邮件也包括您的邮件列表信息，请选择此项。

*在存档中也包含 **MultiPOP** 收集的邮件*

如果您希望存档邮件包括通过 MDaemon 的 MutltiPOP 功能收集到的邮件，请选择此项。

在邮件主题中使用“(存档副本)”标记备份邮件

如果您希望在主题中：档案邮件的邮件头中包含“(存档副本)”，请启用这个选择

存档致公用文件夹（仅限 **MDAEMON** 专业版）

存档接收邮件

点击此复选框，在邮件存档公共文件夹中保存所有的进入邮件。通过默认值，此文件夹只能被邮件管理员通过 IMAP 方式进入。如果您想改变许可或者准予访问给更多的用户，您可以从公共文件夹对话框上的访问控制列表进行设置。

***..**基于接收者地址存档*

如果您希望所有进入邮件存档通过收件人电子邮件地址分类，请点击此选项。

存档发送邮件

点击此对话框，在邮件存档公共文件夹中保存所有出站邮件的拷贝。如果您想改变许可或者准予访问给更多的用户，您可以从公共文件夹对话框上的访问控制列表进行设置。

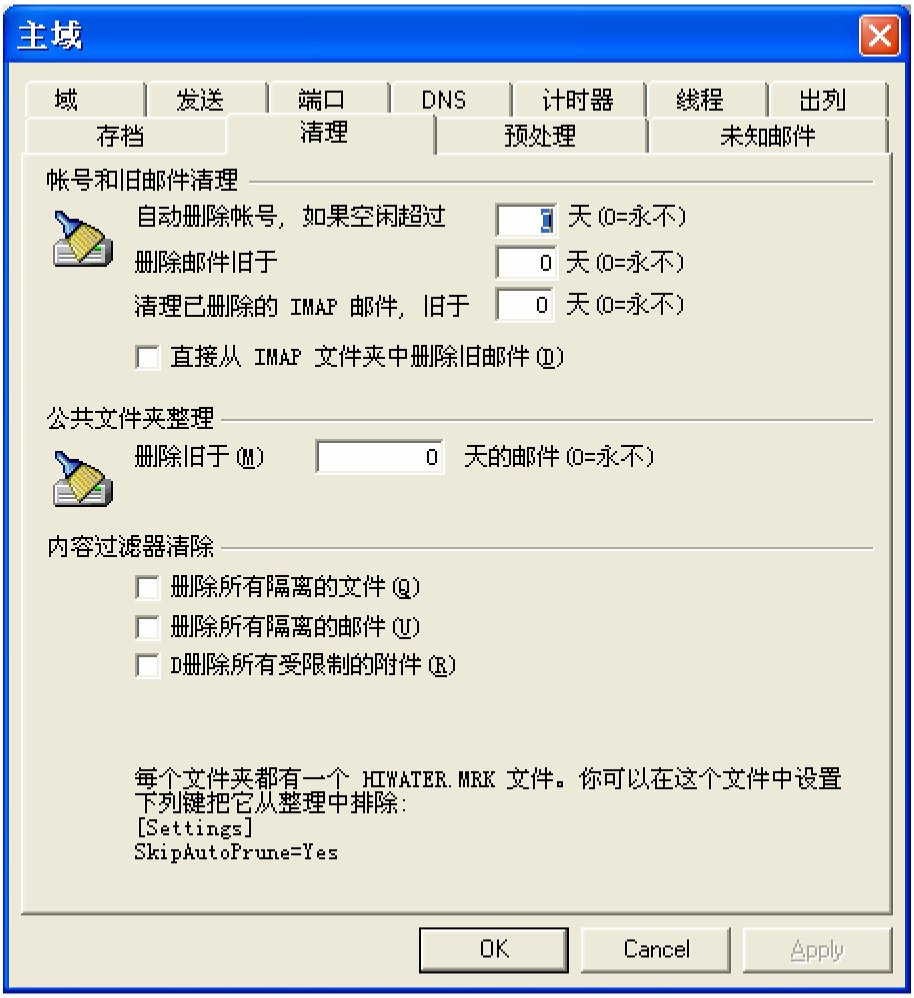
***..**基于发送者地址存档*

如果您希望所有出站邮件存档通过收件人电子邮件地址分类，请点击此选项。

*对每个 **MDaemon** 域提供分开的存档*

如果您希望为每一个域都有用单独的存档，请点击此对话框。

修剪



这个对话框中第一部分的选项是用来指定何时或者是否属于这个域不活动帐号或者老信息将会被 MDaemon 删除。每天午夜，MDaemon 将会删除所有超过规定时间限制的所有信息和账户。在次域对话框上，有类似的用来设置其他域这些限制的控制。在帐号编辑器上，也有用来为个人帐号重设这些设置的控制（参看 305 页）。保留的选项是全局性的，应用到所有域。

> **注意：**
>
> 当旧信息被清理时，不是真正的删除它们，MDaemon 将会把它们移动到“…\BADMSGS\[Mailbox]\”文件夹，这里可以通过管理员或者夜间处理过程被手动删除。**<u>注意：</u>这只能应用到清理旧信息。**当一个帐号被清理时，它的信息都将被单独的删除而不是移动。更多信息和命令行选项，请参看“…MDaemon\App\”文件夹下的 AccountPrune.txt。

帐号和旧邮件清理

<u>自动删除账号，如果空闲超过 xx 天（0=永不）</u>

指定您希望允许属于此域的帐号在被删除前成为不活动状态的天数。在此控制中的值“0”意味着帐号不会因为它们的不活动而被删除。

*删除邮件旧于 **xx** 天（**0**=永不）*
在此控制中指定的值是任意在用户邮箱中邮件，在被 MDaemon 自动删除前的天数。在此控制中的值“0”意味着邮件不会因为它们的过期而被删除。

*清理已删除的 **IMAP** 邮件，旧于 **xx** 天（**0**=永不）*
使用这个控制指定您希望允许已被做删除标记的 IMAP 信息在您的用户文件夹中保留的天数。超过这个天数的做删除标记的消息都将会从他们的邮箱中删除。在此控制中的值“0”意味着做删除标记消息不会因为它们的过期而被清除。

*直接从 **IMAP** 文件夹中删除旧邮件*
如果您想让“删除超过…邮件”控制应用到在 IMAP 文件夹中的信息，点击此检查框。当这个控制停用时，包含在 IMAP 文件夹中的信息将不会被删除，不论它们的时间。

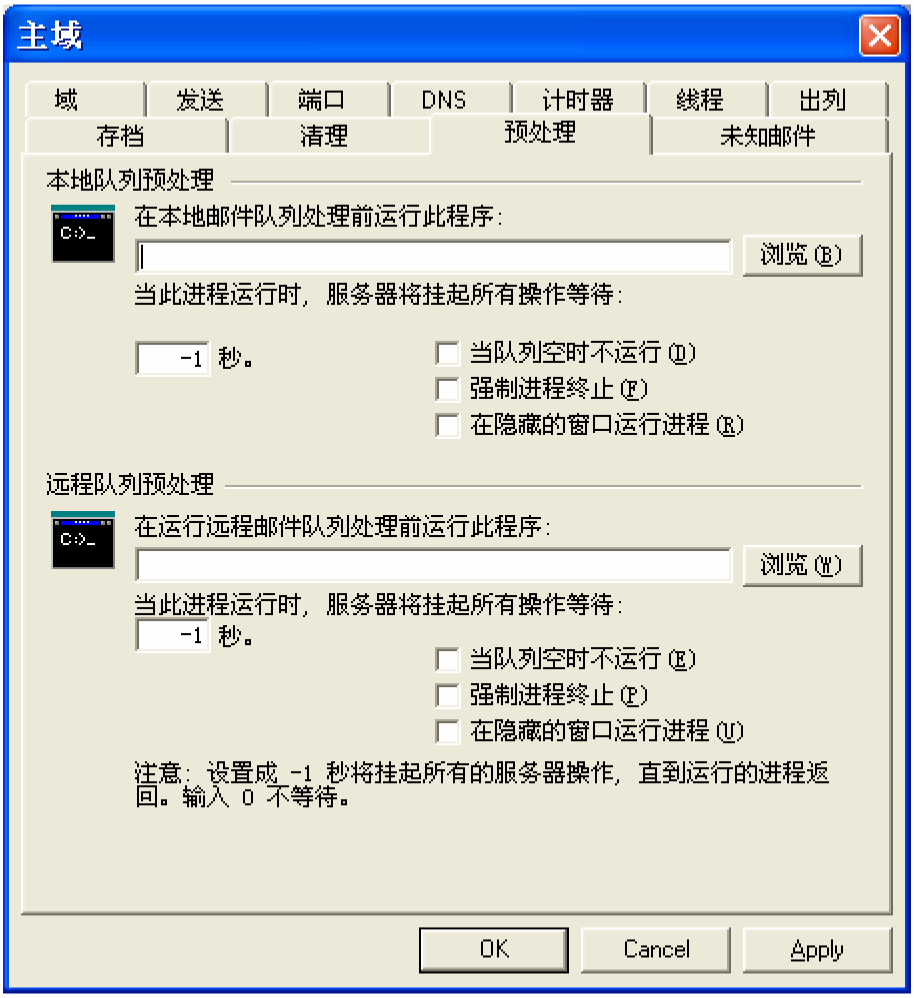
公共文件夹清理
*删除旧于 **xx** 天的邮件（**0**=永不）*
如果您想从公共文件夹中删除老信息，请在此控制中指定天数。

内容过滤器的清除
删除所有隔离的文件
如果您想每个晚上删除所有被隔离的文件附件，请点击此选项。

删除所有隔离的邮件
如果您想每个晚上删除所有被隔离的邮件，请点击此选项。

删除所有受限制的附件
如果您想每个晚上删除所有限定的附件，请点击此选项。

预处理



本地/远程队列预处理

<u>在（本地/远程）邮件队列处理前运行此程序</u>

这个区域指定了在处理或投递任何可能在本地或者远程信息队列中的 RFC-822 邮件过程前被执行的项目路径和名称。如果没有提供完整的路径信息，MDaemon 将会在自己的目录里面，在 Windows 系统目录中，Windows 的下一级目录中首先搜索可执行的，最终目录将被列到路径环境变量中。

<u>…当此进程运行时，服务器将挂起所有操作等待 xx 秒</u>

输入的值决定了当指定项目进行中时，MDaemon 如何运行。当等待运行线程返回时，MDaemon 可以被设置成在指定的时间暂停它的进程。如果在指定时间过去前，线程返回，MDaemon 将立即恢复它的执行线程。在控制中，输入数字 0，MDaemon 将不再挂起操作。输入数字“-1”，将会使 MDaemon 等待直到处理返回，无论经过多长时间。

<u>当队列空时不运行</u>

如果在队列为空时，您不想指定的项目运行，请点击此项。

<u>强制进程终止</u>

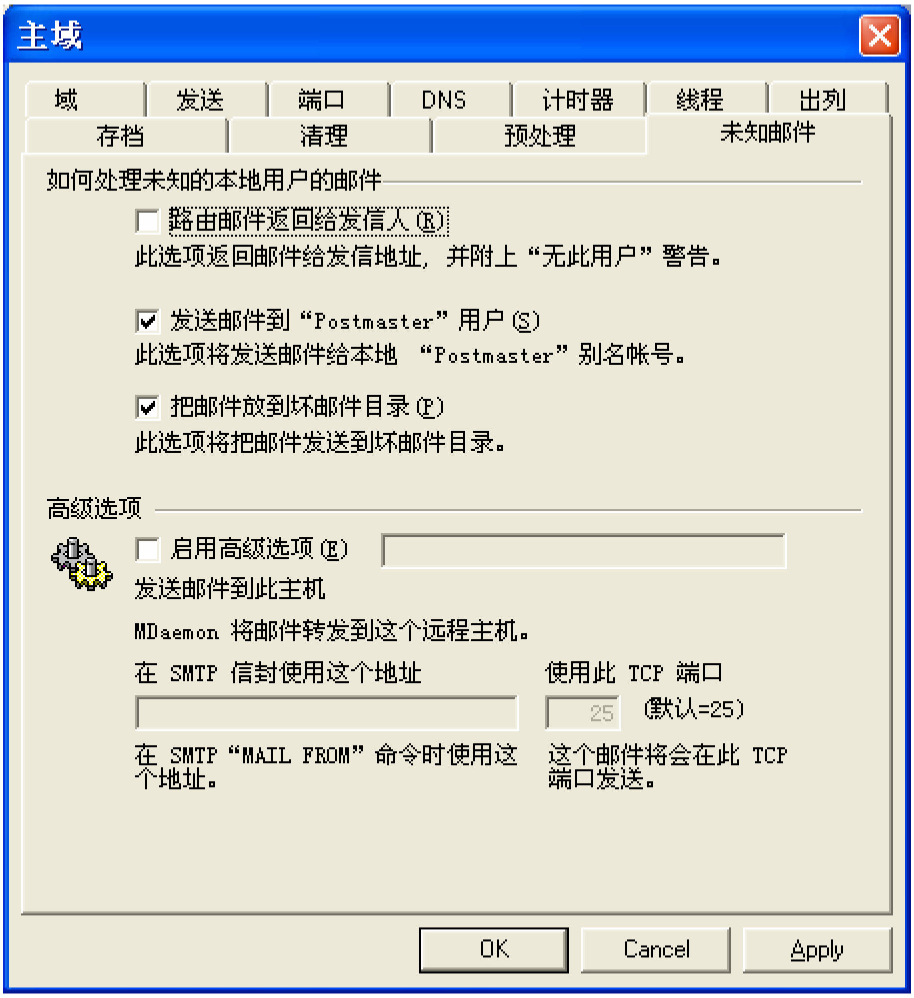
有时，您需要运行的进程自己不会终结。一旦在***<u>…当此进程运行时，服务器将挂</u>***

起所有操作等待 ***xx*** *秒*中的指定时间过去，这个开关将会使 MDaemon 强迫进程终结。如果过去的时间间隔被设置成“-1”，那么此开关不再工作。

在隐藏的窗口运行进程

如果您希望进行载隐藏窗口中运行，请点击此检查框。

未知邮件



如何处理未知的本地用户的邮件

路由邮件返回给发信人

如果此选项激活的话，那么未知的，但被怀疑为本地用户的，到达服务器的邮件将会被返回到邮件的发送者。

发送邮件到“**Postmaster**”用户

无论用户是不是别名为 **Postmaster**，未知的，但被怀疑为本地用户的，到达服务器的邮件将会返回到邮件的发送者。

把邮件放到坏邮件目录

未知的，但被怀疑为本地用户的，到达服务器的邮件将会被路由到坏邮件目录中。

高级选项

启用高级选项

点击检查框，启用以下高级邮件路由属性。

发送邮件到此主机

如果在这里指定邮件主机，地址为未知的本地用户的邮件将会被发送过去。

在 SMTP 信封使用这个地址

在 SMTP“MAIL FROM:”命令中使用的此地址将会用于与接受的主机间的会话。正常的话，消息的发送者将会用于 SMTP 信封的这个部分。如果您需要空命令（MAIL FROM < >），请输入“[Trash]”到此控制中。

使用此 TCP 端口

MDaemon 将会在这里指定的 TCP 端口上发送消息，而不是默认的 SMTP 出站端口。

第四章

MDaemon® 中文版

次域

用MDaemon管理另外的域

运行多个域（仅限MDaemon专业版）

MDaemon版本8包括对多个域的全面支持。除了对主域配置的设定（36页），它包括了用于指定任何数量的附加域的次域编辑器，Mdaemon 支持绑定指定的IP或绑定多个IP地址。

为了支持多重绑定（多个不同的域共享一个IP），Mdaemon自动侦测一个进来的连接试图访问的域名所关联的 IP 地址。举例，假想您有以下的域，并且配置了帐号：

```
altn.com, IP = 1.1.1.1
user-1@altn.com, logon = user-1, POP password = ALTN
arvelh.com - 2.2.2.2
user-2@arvelh.com, logon = user-2, POP password = ARVELH
```

如果一个连接试图访问 1.1.1.1，Mdaemon 会以 altn.com 来响应，如果一个连接访问 2.2.2.2，Mdaemon 会以 arvelh.com 来响应。

如果 user-1@altn.com 来登陆邮箱，他会提供 user-1 作为他的登陆名，ALTN 为密码，来登陆。然而，如果 user-2@arvelh.com 连接 1.1.1.1 来登陆邮箱，那么从技术上来说，他连上了一个错误的服务器（他应该连 2.2.2.2）。在那种情况下，他必须提供他的地址全名来登陆。当然，如果他连上 2.2.2.2，只需要提供用户名就可以了。因此，如果一个帐号连上了和域名对应的 IP 地址，而且此 IP 地址和没有被其他域所使用，那么此帐号只需要提供用户名就可以了，否则，就必须指定一个完整的邮件地址。在这种情况下，支持多个域关联一个 IP 地址。当多个域关联一个 IP 地址，登陆名字就必须包含一个完整的邮件地址。否则 Mdaemon 就不知道哪个用户在试图登陆，如果存在不确定性，就最好使用完整的邮件地址来登陆。

那么如果指定登陆和域呢？您期望提供类似于这样的账户电子邮件地址：arvel@altn.com。MDaemon总是会接受包含‘@’标志的登陆信息。因此如果您的邮件客户端在登陆值中支持使用‘@’标志，那么就没有任何问题。然而在今天市场中的许多邮件客户端都关掉了此功能，将不允许在登陆区域内使用‘@’标志。为了供应那些不支持此功能的邮件客户端，MDaemon允许您指定一个可选择的字符。MDaemon 默认选择字符是‘$’。这意味着您可以使用：像 arvel@altn.com 一样简单的 arvel$altn.com.

在杂项对话框上的系统标签指定可选择字符（269页）。此值可以设置到10个字符以上，使得提供字符串作为分隔符来替换单独字符，例如‘$’成为可能。例如，使用‘.at.’将允许您使用“arvel.at.altn.com”作为登陆值。

几个关键功能，比如账户，列表，和安全功能，都是基于每一个域基础上的。当您创建邮件帐号的时候，您必须指定新帐号属于的域。同样对邮件列表也一样。

这意味着 IP 屏蔽和 IP 保护这些功能将各别的受到域的约束。然而，一些功能，比如 DomainPOP“真实名称匹配”功能，只受到主域的约束。

作为多域处理过程的一部分，当您创建一个次域的时候，以下别名将会自动被设置成：

MDaemon@scondarydomain.com=MDaemon@primarydomain.com
listserv@secondarydomain.com=MDaemon@primarydomain.com
listserver@secondarydomain.com=MDaemon@primarydomain.com
list-serv@secondarydomain.com=MDaemon@primarydomain.com

如果次域被删除，这些别名也将被自动删除。

次域编辑器

MDaemon 服务器全面支持多域。除了主域配置设定中（36 页），它包含次域编辑器用来配置任意数量的次域。MDaemon 支持单一的（静态的）和多本地 IP 地址。

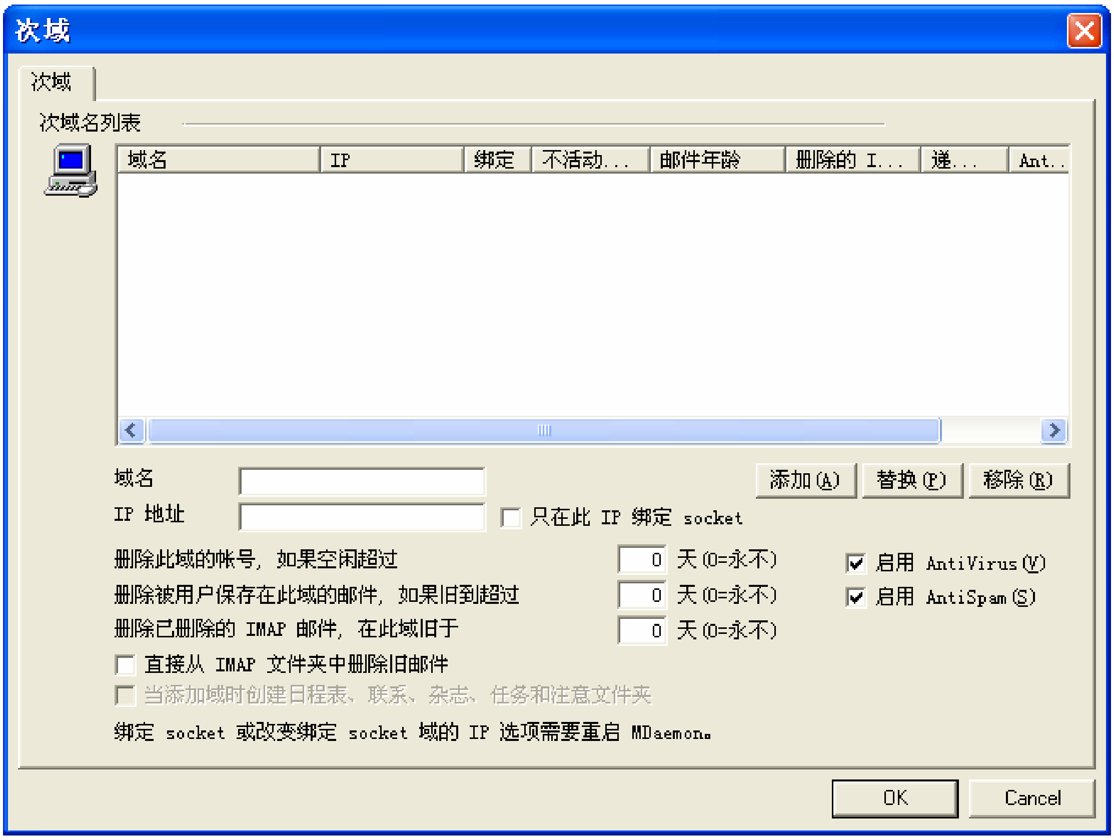
在次域编辑器中，对于每一个次域，您应该包括：域名称，与之相关联的 IP 地址，以及是否和 IP 绑定。

运行多个域，更多信息请参看：

运行多个域-64 页

也可以参看

主域配置-36 页
账户编辑器-295 页



次域名列表

此窗口包括了您的次域。它有几个专栏：域名称-列出每个域的名称，IP-每个域

的 IP 地址，绑定-显示是否给定的域和它的 IP 地址绑定，在列表下面的其他几个栏目是与此控制关联的。简单点击您希望排列列表的专栏，然后就会以升序排列专栏。再次点击相同的专栏，便会以降序排列。

域名

输入您希望运行的次域的域名称。

IP 地址

输入与添加或编辑域相关联的 IP 地址。

*只在此 **IP** 绑定 **socket***

如果您希望捆绑次域到它的 IP，请点击此检查框。

添加

点击此按钮连同 IP 地址添加次域，并且绑定状态到域列表。

替换

当您点击域列表中的一个输入时，它的设置将会出现在相关控制中。在生成任何需要信息的改变后，点击此按钮用新设置替换原来的输入。

帐号和旧邮件清理

如果您希望个人设置替代默认值，那么这个对话框中保留得三个控制在会被用到，账户管理器上（305 页）都有相应的控制。

*删除此域的帐号，如果空闲超过 **xx** 天（**0**=永不）*

指定您希望允许属于此域的帐号在被删除前不活动的天数。这个控制里面的值“0”表示帐号不会因为处于不活动状态被删除。

*删除被用户保存在此域的邮件，如果就到超过 **xx** 天（**0**=永不）*

在此控制中指定的值是在 MDaemon 自动删除前，任意给定的邮件可以在用户邮箱中存在的天数。值“0”表示邮件不会因为时期被删除。

*删除已删除的 **IMAP** 邮件，在此域旧于 **xx** 天（**0**=永不）*

使用此控制指定您希望允许 IMAP 邮件被做上删除标记在此域的用户的文件夹中保留的天数。做上删除记号的消息长过这个天数将会被从他们的邮箱中清除。

*直接从 **IMAP** 文件夹中删除旧邮件*

如果您希望在 IMAP 中也对邮件应用“删除被用户保存在此域的邮件…”控制。当这个控制停用的时候，IMAP 文件夹中包含的消息将不会被删除，不论他们的日期。

注意：
当旧邮件被清除的时候，而不是真正的删除它们，MDaemon 将会把它们移动到“…\BADMSGS\[Mailbox]\”文件夹中，这里

> 可以被管理员或者夜间处理过程手动的删除。此功能只应用到被清除的旧邮件-当一个帐号被修建时，它和它的邮件将被单独地删除，而不是移动。更多信息和命令行选项，请在“…MDaemon\App\”文件夹中参看 AccountPrune.txt。

当添加域时创建日程表、联系、杂志、任务和注意文件夹
如果您希望无论何时添加次域，都可以自动创建这些组件文件夹，请点击此检查框。

启用 AntiVirus
如果安装了 MDaemon 的反病毒，如果您希望反病毒设置应用到选择的次域，那么请点击此检查框。

启用 AntiSpam
如果您希望 MDaemon 当前的垃圾邮件过滤器设置应用到选择次域，那么请点击此检查框。

添加次域

添加次域到域列表：

1、 输入域名和 IP 地址
2、 点击只在此 IP 绑定 socket（指在您希望绑定域到它的 IP）
3、 点击添加

编辑次域

编辑次域

1、 点击您希望编辑的域列表
2、 将需要的在控制中出现的信息变更
3、 点击替换

移除次域

移除次域

1、 点击您希望从域列表中移除的输入
2、 点击移除

第五章

MDaemon® 中文版

远程配置

使用WebAdmin，配置远程配置

WebAdmin 是为 Alt-N Technologies 公司提供基于网络远程管理支持的应用程序。WebAdmin 包括对 Alt-N 的 Windows 版 MDaemon®服务器的广泛支持，以及 MDaemon 整合的网络基础的电子邮件组件，WorldClient®。

WebAdmin 是一个被设计在相同计算机上后台运行的服务器应用程序，作为管理 Alt-N Technologies 软件。连入 WebAdmin，您简单的打开您的浏览器，并将它指向 URL，和 WebAdmin 存在的端口号（例如，www.mywebadmin.com:1000）。在提供您的登陆认证后，您将被赋予控制和设置 MDaemon 和其它 Alt-N 产品的权限。您所访问的设置的类型和数量依赖于连接的级别。有三个访问级别可以提供给 WebAdmin 用户：全局。域和用户。

- 全局管理员 – 全局管理员是那些拥有全局访问许可的用户，可以在 MDaemon 帐号设置下启用。全局访问意味着用户可以通过 WebAdmin 查看和设置任何可被访问的配置。全局管理员可以添加，编辑，和删除用户，域和邮件列表。他们可以编辑产品的 INI 文件，制定其它的用户称为域管理员，管理密码，以及做许多其它事情；他们拥有完全的管理控制权

- 域管理员 – 类似于全局管理员，域管理员通过 WebAdmin 拥有对所有用户和可访问产品设置的完全管理权。然而，他们的管理控制权是受到域或者他们被给定访问的域的限制。域管理员和他们所控制的域是从 WebAdmin 中通过全局管理员指定的，或者通过另外一个域管理员准许进入那些域。

- 用户 – WebAdmin 访问中最低级别的是用户访问。例如来说，MDaemon 可以登录到 WebAdmin，并查看他们个人的帐号设置以及编辑他们的 MultiPOP 输入，IMAP 过滤器，自动回复，及其它。可被编辑的此设置的类型和数量依赖于给定的每一个用户的个人账户设置的许可。

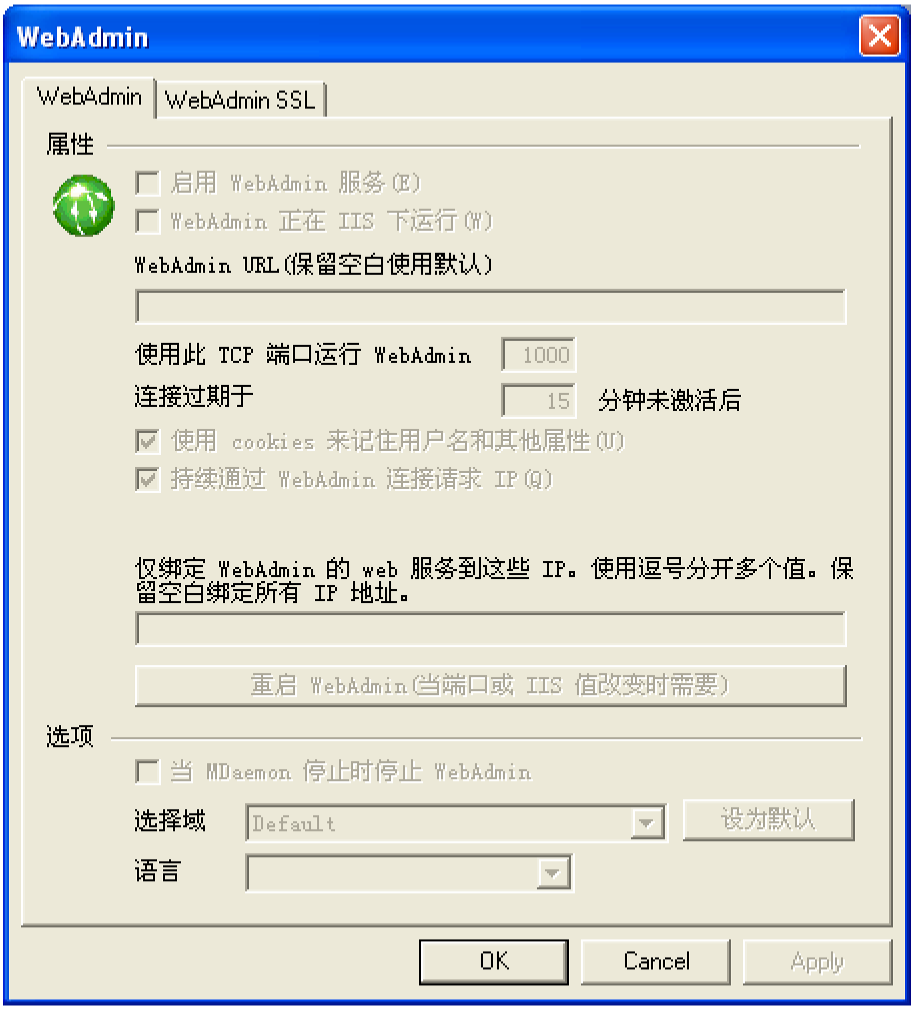
注意：
WebAdmin 并不是随着 MDaemon 服务器被默认安装的。它是一个免费的插件，可以从 Alt-N Technologies 的网站 www.altn.com 上获得。

WebAdmin 的更多信息，请参看：

WebAccess 默认 – 291 页
帐号编辑器 → Web – 309 页

Web 完整的信息，请参看 WebAdmin 用户手册。您可以从 www.altn.com 上获得此手册。

WebAdmin



属性

<u>启用 WebAdmin 服务</u>

点击此复选框启用 WebAdmin 服务。您可以从 MDaemon 主 GUI 文件菜单中或者统计表和快捷方式框架，启用/停用 WebAdmin。

<u>WebAdmin 正在 IIS 下运行</u>

在 IIS 下，而不是内建网络服务器运行 WebAdmin 时，点击复选框。这可以阻止可能会导致和 IIS 的冲突的某些 GUI 元素的访问。

更多信息，请参看*在 IIS 下运行 WebAdmin* – 72 页。

<u>使用此 TCP 端口运行 WebAdmin</u>

WebAdmin 将会监听此端口来响应您的网络浏览器中的连接。

连接过期于 xx 分钟未活动

当您登陆到 WebAdmin 时，这个值是允许您的会话在 WebAdmin 关闭它之前可以成为不活动状态的时间。

使用 cookies 来记住用户名和其它属性

如果您希望 WebAdmin 在您本地的计算机上的缓存中存储您的登陆名和某些其它的功能，点击此选项。

持续通过 WebAdmin 连接请求 IP

作为一个附加的安全方法，在会话开始时，您可以点击此复选框使得 WebAdmin 限定每一个会话到您连接的 IP 地址。因此，从被需求的 IP 持续，没有一个人可以“偷窃”通话。这个配置更安全，而不会导致如果您使用代理服务器或者拨号帐号动态分配和改变 IP 地址的问题。

使用 HTTP 压缩

如果您希望在 WebAdmin 通话中使用 HTTP 压缩，点击此复选框。

仅绑定 WebAdmin 的 web 服务到这些 IP

如果您需要限制 WebAdmin 服务器到某些 IP 地址，通过逗号在此制定哪些 IP。如果您对此区域留空，之后，WebAdmin 将会检测所有您为您的主要和次域制定的 IP 地址。

重启 WebAdmin（当端口或 IIS 值改变时需要）

如果您希望重新启动 WebAdmin 服务器，点击此按钮。注意：当改变端口设置时，为了新设置被识别，您必须重新启动 WebAdmin。

在IIS下运行WebAdmin

WebAdmin 被配备在内建的网络服务器中，以此执行时不需要 IIS。但是，它支持 IIS，因此也就可以实现作为 ISAPI DLL 的功能。

注意：
当在 IIS 下，运行 WebAdmin 时，您将不能再从 MDaemon 的界面中开始或者停止它。您必须使用 IIS 提供的工具才可以。

在 IIS 下配置 WebAdmin 3.x

1. 如果 WebAdmin 没有安装，在安装时请选择此选项，“**我希望为 WebAdmin 使用其它的 WEB 服务器**”。如果 WebAdmin 已经被安装，请在 Windows 开始菜单的 WebAdmin 组中，使用“停止 WebAdmin”或者从 MDaemon 的界面中停止 WebAdmin。
2. 打开 IIS 管理项目
   （**开始 – 设置 - 控制面板 - 管理工具 - Internet 服务管理器**）

3. 右击默认站点，然后选择新建 – 虚拟目录
4. 根据向导指领您的步骤创建虚拟目录。下面是建议输入到向导中的名字和数据位置，但会根据您的 MDaemon 和 WebAdmin 的安装位置有所改变。
   A．别名：“WebAdmin”，点击下一步
   B．目录：“c:\MDaemon\webadmin\templates”，点击下一步
   C．点击下一步
   D．点击完成
5. 设置执行许可到脚本
6. 设置应用程序保护级别为低（**IIS** 进程）
7. 在虚拟目录标签上的应用程序设置部分点击配置按钮
8. 在映射标签上点击添加
9. 在可执行区域，输入“c:\MDaemon\webadmin\template\webadmin.dll”。注意：这个区域不能包括空格。如果路径中包括空格，则必须转换成 8.3 格式。Dir /x 命令可以显示文件或者目录的 8.3 名称。
10. 在扩展名区域内输入“.wdm”并且选择全部动作。
11. 点击脚本引擎栏
12. 点击 **OK**
13. 如果您选择的话，所有其它的映射都将被移除，之后点击 **OK**
14. 在文档标签上添加 login.wdm 作为默认文档，并从列表中移除所有其他的条目。
15. 在 MDaemon 中，到设置 – **WebAdmin…**并点击启用 **WebAdmin** 服务器和在 **IIS** 下运行 **WebAdmin**。
16. 在 **WebAdmin URL** 中输入“/WebAdmin/login.wdm”
17. 点击 **OK**

在 IIS 6 下配置 WebAdmin 3.x

为 WebAdmin 创建一个新的应用程序池：

1、如果还没有安装 WebAdmin，之后在安装中选择选项，“我希望为 **WebAdmin** 使用另一个网络服务器”。如果 WebAdmin 已经安装了，在 Windows 开始菜单下，WebAdmin 组中使用“停止 **WebAdmin**”停止。

2、打开 IIS 管理项目（开始 - 设置 – 控制面板 – 管理工具 – **Internet** 服务管理器）。

3、右击应用程序池。

4、 点击新建 – 应用程序 **Pool**

5、在应用程序 Pool ID 区域键入“Alt-N”并点击 **OK**

6、右击 **Alt-N**

7、点击属性

8、点击性能标签

9、清除“在空闲后关闭工作进程”和“限制内核请求队列”。

10、 点击标识标签

11、 在下拉框中，选择本地系统。

12、 点击 **OK**

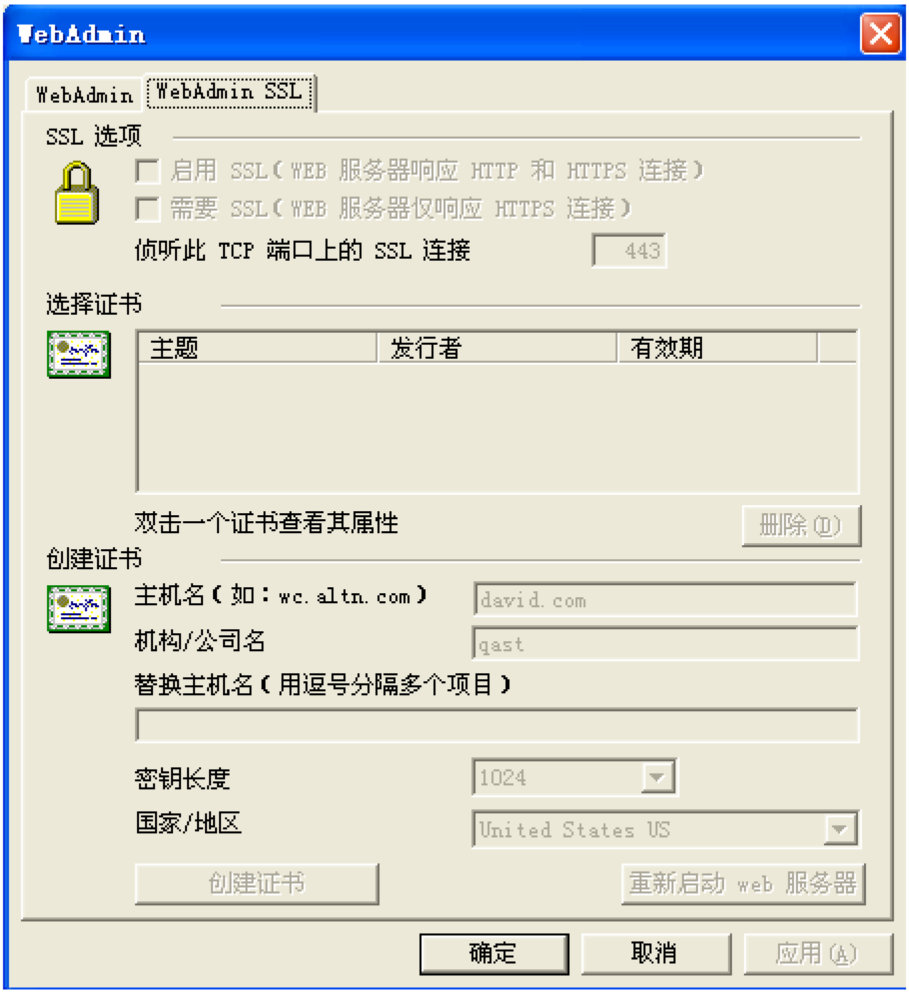
为 **WebAdmin** 创建虚拟文件夹

1、打开 IIS 管理项目（开始 - 设置 – 控制面板 – 管理工具 – **Internet** 服务管理器）。
2、右击您的网页并且选择新建 – 虚拟目录。
3、为虚拟目录指定别名（例如，“WebAdmin”）。
4、在路径区域，键入 WebAdmin 临时目录的路径 – 例如，“c:\program files\alt-n technologies\webadmin\templates”。
5、钩选读取和运行脚本选项。
6、关闭向导并且右击创建的虚拟目录。
7、选择属性。
8、在本地目录标签上，改变 Alt-N 的应用程序 Pool。
9、点击配置按钮。
10、 点击添加，添加一个 ISAPI 扩展映射
11、 在可执行区域输入文件 WebAdmin.dll 的路径。例如，“C:\Program Files\Alt-N\WebAdmin\Templates\WebAdmin.dll”。
12、 在扩展名区域输入“.wdm”。
13、 点击脚本引擎和确认文件是否存在。
14、 点击 **OK**。
15、 如果您选择，所有其它的影射都将被移除，然后点击 **OK**。
16、 选择文档标签。
17、 确定钩选启用默认内容页
18、 确定只有“login.wdm”存在队列中。
19、 点击 **OK**，并退出虚拟目录属性对话框。

添加.WDM 到允许网络扩展列表

1、点击 WEB 服务扩展文件夹（在 IIS MMC 中）
2、点击添加新 **WEB** 服务扩展
3、在扩展名区域输入“WebAdmin”。
4、点击添加，然后浏览 WebAdmin ISAPI 扩展。例如：C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll。
5、检查设置扩展状态为允许
6、 点击 **OK**
7、 在 MDaemon 中，到设置 **– WebAdmin…**并点击启用 **WebAdmin** 服务器和在 **IIS** 下运行 **WebAdmin**
8、在 WebAdmin URL 中键入“/WebAdmin/login.wdm”
9、点击 **OK**

WebAdmin SSL



WebAdmin 的 WEB 服务器支持 SSL 协议。Netscape Communications Corporation 所发展的 SSL 协议是保护服务器/客户端网络通讯的标准方法。它提供了对 TCP/IP 连接的服务器认证，数据编码，以及可选的客户端认证。而且因为由于 SSL 被内建到了当前所有主流的浏览器中，因此在您的服务器上，简单的安全安装一个合理数字认证将会激活连接客户端的 SSL 能力。如果您不选择在 IIS 下运行 WebAdmin，那么您可以将这个安全方法直接内建到 WorldClient 中。

注意：
只有当使用 WebAdmin 的内建网络服务器时，才能将此对话框应用到 WebAdmin 中。如果您配置 WebAdmin 使用 IIS 工作替换其自己的网络服务器，则不会使用这些选项 – 必须在 IIS 中设置对 SSL 的配置。

启用和配置 WebAdmin 来使用 SSL 的选项在 SSL & Certificates 对话框上（点击 Ctrl+L 或安全 – SSL/TLS/证书… - WebAdmin SSL）。然而，为了您的方便，这些选项在 WebAdmin 对话框中是可利用的。

此对话框更多信息请参看 159 页

SSL & Certificates 更多信息请参看 153 页

第六章

MDaemon ® 中文版

WordClient服务器

设置和使用WorldClient服务器

概述

WorldClient 包含于 MDaemon v8 中。WorldClient 是设计用来让用户使用他们自己喜欢的 WEB 浏览器得到邮件客户端功能的这样一个基于 WEB 的电子邮件解决方案。所有他们的邮件文件夹都将存放于服务器上，这样就可以使得他们就像在办公室里面一样，在任何地方访问任何东西。在提供它自身能力的附加优点以保证用户可以任何时间任何地点访问他们的电子邮件时，相对传统邮件客户端而言，WorldClient 可以很轻松的控制。

有许多使用 WorldClient 的途径。使用它可以让您的移动办公人员可以使用到他们的电子邮件 – 记得，WorldClient 并不依赖工作站，因此“Mobile”也意味着仅在建筑间传递。使用 WorldClient 给您的客户提供基于 WEB 的电子邮件服务，以及自定义显示广告条的界面。在公共电脑或者计算机实验室时使用它提供电子邮件给学生或者其他可能不拥有个人计算机的其它人群。

WorldClient 也为邮件管理员提供便利。自从 WorldClient 不再依赖工作站，您就不必配置和保留个人邮件客户端。在 WorldClient 自定义图形图片和 HTML 页，以适应您的全体或者您的客户的需求。而且，给您的用户权利来维持他们自己的帐号设置，这样可以节省您的时间 – 您可以为您的用户或多或少的控制权限。

最后，一些功能将直接使您的客户受益，比如：无论何处您找到一个浏览器，都提供扩展功能的电子邮件，可使用 18 种语言的客户端界面，个人和全局地址薄，管理邮件文件夹以及过滤器，发送或者接受文件附件，对于界面的多个可视化主题，以及更多。

日历和日程系统

MDaemon 拥有一套完整的整合日历和时间日程系统，这个系统可以主要通过 WorldClient 进行访问和控制。日历系统可以用来为您和您的域客户提供发送便签和日程表，查看约会和会议。约会和会议可以指定为公共的或者私人的，您拥有对访问许可完全控制。通过从一个下拉列表中选择的用户能够，您可以看到用户的日历和查看所有您允许访问的事件。如果您被赋予了到用户日历的写 – 访问权限，您甚至可以为他们安排日程表。

由于日历系统是整合到 MDaemon 中的，因此对会议的电子邮件通知和第三方安排的约会都会有许多添加的便利。无论何时，其他人为您安排了一个约会，

您将受到一封电子邮件信息，其中概括了这个约会。对于会议，每一个指定的会议参与者都将受到一封关于会议日期，时间，地点，主题和参与者列表细节的电子邮件信息。而且，在安排上与会议时间档有冲突的与会者，都将受到一封提醒他们会议和时间表上安排冲突的提示。而安排会议的人将会受到一封所有会议细节和可以参加会议或因安排有冲突不能参加的邀请人的名单。最后，使用日历的自动日程安排功能，可以通过日历系统搜索最靠前且无安排上冲突的事件空档，来完全的避免冲突。之后，您可以接受建议的事件空档也可以选择一个新的。

日历系统也支持 Microsoft Outlook 使用的 Internet 日历（iCal）和其他电子邮件程序所适用的 iCalendar。日历系统可以检测并执行 iCanlendar 信息发送到您的用户，从而升级他们的日历。当一个用户从 WorldClient 中打开一个 iCalendar 附件时，附件中包含的信息将会反映到用户的 WorldClient 日历中。而且，当用户创建新的会议或者约会时，他们可以列出一个或者多个他们希望发送 iCalendar 电子邮件的地址。这个性能可以在每一个域基础上进行设置，让个人用户在他们 WorldClient 设置中人工代替它们。

日历系统也可以用来发送全局备忘录（在每一个用户的日历中将出现备忘录）。通过创建一份备忘录，然后点击复选框，这个功能也可以用发布一份给全体域组成员的提示。另外，为了更多的安全性和多功能性，在 MDaemon 中可以对创建和查看全局备忘录进行完全的控制。这些控制位于 MDaemon 中的 WorldClient 对话框的 WorldClient 日历标签中（设置 – WorldClient – WorldClient 的日程表）。您可以准许读或者写权限给所有的域用户，或者不给，再或者指定的个人。这些权限都是基于每一个域进行控制的。

除了控制全局备忘录权限外，日历和日程安排对话框也可以用来为每一个单独的域，完全启用和停用日历系统。因此，您可以提供给日历功能尽可能多或者尽可能少的，使您满意创建的域。

ComAgent

MDaemon 配备了 ComAgent，一套安全即时消息系统，地址薄客户端，和提供快速访问 WorldClient 电子邮件功能的托盘 java 程序。WorldClient 用户可以下载 ComAgent，之后安装到个人用户的本地计算机上。对于特殊用户，在下载时，可以预配置它，可以限制手动配置的需求。

在后台运行的 ComAgent，会通过直接询问 WorldClient 服务器来检查您帐号中的新邮件。这样可以消除需要打开一个浏览器或者保持一个浏览器以检查您的电子邮件 – ComAgent 会检查新邮件并且当有新邮件到达时，用声响或者可视化提示来提醒您。ComAgent 也会显示一个您的电子邮件文件夹列表和每一个文件夹所含的消息的数量和类型（新，未读，已读）。而且，它可以用来启动您的浏览器，并且即刻将它移动到一个指定的邮件文件夹，第一封未读邮件，编写页，或者日历页中。

另外，当您使用 Alt-N 的“LDaemon”LDAP 服务器来维持 WorldClient 的公共和私人文件夹时，ComAgent 可以在每一个用户本地计算机上的 LDaemon 和 Outlook/Outlook Express 地址薄间，提供双通路同步。因此，如果您在不同的时间内使用 Outlook 或者 Outlook Express 和 WorldClient，在所有产品中，将会匹配地址薄。最后，ComAgent 配置了一套完整即时消息系统。您可以查看您 ComAgent“密友”和每一个在线状态（在线，离开，离线）的列表，开始任意

成员或者一组成员的对话，设置您自己的在线状态，以及查看在历史文件夹中取得通话记录。更多关于如何使用 ComAgent 的特殊指令，请查看它的在线帮助系统。

在域设置标签上有几个关于 ComAgent 和即时消息（IM）的选项。（94 页）

ComAgent的即时消息系统

ComAgent 配置了一个简单但有效的即时消息（IM）系统。利用这个系统，您可以在您的 MDaemon 服务器上，同其他帐号即时的交流。您可以从 MDaemon 用户列表中选择“密友”列表，然后查看谁在线并且已经准备好接受一个即时消息。您可以一次启动包括几个好友在内的一组对话。所有 IM 功能都可以通过 ComAgent 中的快捷（右击）菜单来实现。

ComAgent 的 IM 系统也是可编写的，允许用户程序以之为界面。通过在\MDaemon\WorldClient\目录下创建 SEM 文件，外部应用程序能够立即给 ComAgent 用户发送 IM 消息。以下是 SEM 文件格式：

To: frank@example.com ComAgent用户的电子邮件地址
From: rip@example.com 即时消息发送者的电子邮件地址
<blank line>
即时消息的文本 这是作为即时消息发送的文本

SEM文件名必须字母“IM-”开头，而后面需跟随唯一的数字值。例如，“IM-0001.SEM”。应用程序将会创建一个名为“IM-0001.LCK”的管理文件来锁定SEM文件。一旦完成的SEM文件移除了LCK文件，则SEM文件将会被处理。MDaemon使用此脚本方案发送即使消息来提醒您即将到来的约会和会议。

使用此脚本方案来发送即时消息这个操作将会被添加到内容过滤器系统中。而且，规则来利用此操作可以在IM中使用内容过滤器宏。例如，您可以建议一个类似于以下例子的即时消息规则

You have received an email from $SENDER$.
Subject: $SUBJECT$

此规则是通过ComAgent得到新邮件提示的一个有效方法。
由于考虑到在集中的固有缺陷，以及传统检测IM通信量和众所周知的IM客户端的不足，许多商业单位和管理员对在他们的公司内部使用即时消息系统持保留意见，因此我们用ComAgent的即时消息系统来弥补这种不足。首先，我们的系统不是点对点的– 个人ComAgent客户端不会直接连接到其他客户端上。而且因为每个IM都要通过服务器，每一个信息都要通过管理员可访问的中心服务器，由于公司和所有雇员的安全因素，所有会话的记都会被保存维护。IM活动的信息都会被记录在MDaemon\LOGS\directory的InstantMessaging.log文件中，对于确保安全的一个主要原因就是我们不支持其他的即时通讯客户端，象ICQ，AOL，和MSN。我们可以在以后的版本中加入此功能。总而言之，我们的即时通讯系统是安全的，因为从始致终，所有传输的信息都是加密的，从来不会传明文的信息。

即时消息是在每个域基础上提供的。对激活即时消息的控制和指定是否为 IM 通信量都将被记录到选项标签的 WorldClient 对话框中（设置 – WorldClient…– 选项）。

自动地址薄同步

通过使用 ComAgen 与 Mdaemon 的集成地址簿系统，您可以在每一个用户的本地计算机上 Outlook/Outlook Express 地址薄和 Mdaemon 之间提供双向同步。因此，如果您不在同时使用 Outlook 或 Outlook Express 和 WorldClient，地址薄将会在以上产品中同步。

每一次 MDaemon 帐号被添加，删除或者调整， MDaemon 能够保持一个精确的和连续的用户数据库的升级。ComAgent 可以在固定的间隔对 MDaemon 进行挂通信而且获得所有储存在那里的联系人信息。它之后会发布这些信息到本地计算机的 Windows 地址薄或者联系人中。此功能将会有即时升级任何使用本地地址薄系统的本地软件包（例如，Outlook/Outlook Express）。

使用 ComAgent 且具有合适的访问证书的任何人可以通过直接使用 Windows 地址薄或借助 Outlook/Outlook Express 添加公共联系人。新建联系人将会被 ComAgent 获得，并上载到 MDaemon。从那里，所有在您的网络上的其它的用户在下一次他们的 ComAgent 联系 MDaemon 时，将可以访问新建联系人。

在同步标签上的 ComAgent 属性对话框，您可以在您的 Windows 地址薄中指定一个文件夹来同步联系人信息，也可以指定不同的文件夹针对公共和私有联系人。

注意：
Windows 地址薄（WAB）同步需要有启用身份支持的 IE5 或者更高版本。

以下地址薄字段将会被同步：

全名
家庭地址
家庭所在城市
家庭所在省
家庭邮编
家庭所在国家
家庭电话
家庭传真
家庭移动电话
家庭主页地址
商业公司
公司地址
公司所在城市
公司所在省
公司邮编
公司所在国家
公司名称
公司部门
公司办公室
公司电话
公司传真
公司传呼

公司IP电话
公司网址
评语

在 MDaemon 和 WorldClient 中各种地址薄选项的更多信息，请参看：

LDAP 选项 – 109 页
杂项选项 – 275 页

使用WorldClient

启动WorldClient

这里有三种方法启动或停止 WorldClient 服务器：

1. 在左侧状态标签上，右击 WorldClient 条目并选择在快捷菜单上的*切换活动/非活动*选项。
2. 在主界面上，点击**文件 – 启用 WorldClient 服务器**。
3. 点击在主界面上的**设置 – WorldClient…**，之后点击在 WEB 服务器标签上的**启用 WorldClient 服务器**。

登入到WorldClient

1. 将您的 Web 浏览器指向 http://main-or-second-domain.com:WCPortNumber。可以在 WorldClient 的对话框的 Web 服务器标签上指定此端口。如果您配置 WorldClient 监听默认网络端口（80 端口），则您不需要在登陆 URL 中指示端口号（例如 www.mydomain.com 替换 www.mydomain.com:3000）。
2. 输入您的 MDaemon 帐号的用户名和密码。
3. 点击**登陆**。

改变WorldClient的端口设置

1. 点击在菜单栏上的**设置 – WorldClient…**。
2. 在控制表示中，在*运行 WorldClient 服务时，使用此 TCP 端口*输入希望的端口值
3. 点击确定

WorldClient文档

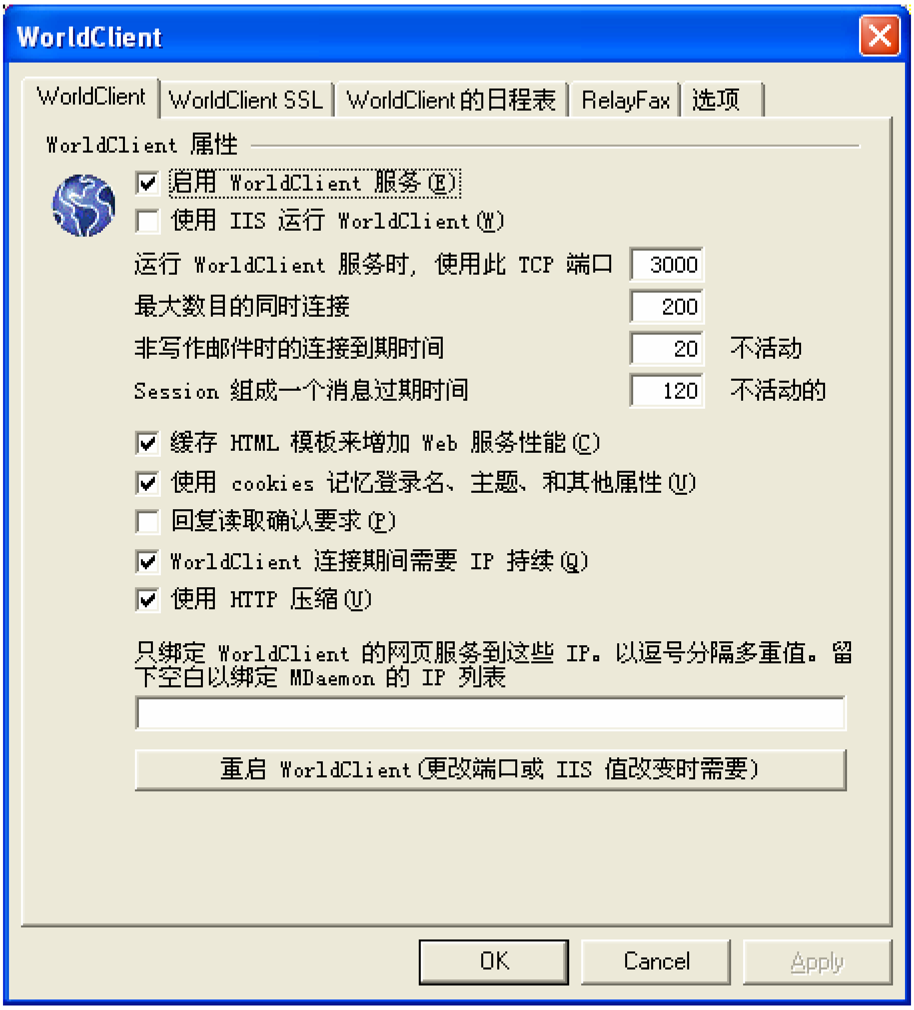
客户端帮助

WorldClient 为您的用户配置了广泛的客户端帮助。客户端功能和功能信息，请参看 WorldClient 中的在线帮助系统。

WorldClient邮件

使用**设置 – WorldClient…**菜单选项来启用您的 WorldClient 服务器，并配置各种 WorldClient 相关设置。您可以指定它监听的端口和您希望在 WorldClient 会话过期前保留活动状态的时间。您也可以控制许多全局或者域的特殊设置，比如：使用的默认语言和主题，用户是否可以创建帐号，邮件列表的默认分页，ComAgent 支持是否启用，是否允许及记录即时消息，许多日历及日程安排功能，公共和私人地址薄设置，传真整合，及更多。

WEB服务器



此标签中包括控制 WorldClient 的配置和行为的各种全局及服务器级别设置，无论它们属于哪个用户或者域。

<u>WorldClient 属性</u>

启用 WorldClient 服务

点击此检查框来启用 WorldClient 服务。您也可以从文件菜单或者统计状态表快捷框架中，启用或者停用 WorldClient。

使用 IIS 运行 WorldClient
当在 IIS 下运行 WorldClient 而不是 WorldClient 内建的 WEB 服务器时，点击此复选框。可以阻止某些 GUI 元素连入，否则，可能会因此导致和 IIS 的冲突。更多信息，请参看*在 IIS 下运行 WorldClient* – 86 页。

运行 WorldClient 服务时，使用此 TCP 端口
这个是 WorldClient 监听您的用户浏览器连接所用的端口。

最大数目的同时连接
这是用户同时连接到 WorldClient 的会话的最大数

非写作邮件时的连接过期时间
当一个用户登录到 WorldClient 中，但没有编写消息，这个量就是他们的会话在 WorldClient 关闭它前，保留不活动的时间。

撰写一个邮件时，会话过期时间
这个计时器控制的是当用户编写消息时，会话保持打开状态的时间，以及通话保持不活动。当用户编写邮件时，将此计时器设置比*非编写消息的通话*…计时器稍高些是非常好的。指示因为编写消息直到发送出，都不需要与服务器通信。

缓存 HTML 模板来增加 Web 服务性能
点击此栏可以使 WorldClient 将模板存贮到内存中，而不是每次当需要连接它们的再读入。这样可以显著的提高服务性能，但如果您对模板文件之一作出了改动的话，您将不得不重启 WorldClient。

使用 Cookie 记忆登录名，主题和其他属性
如果您希望 WorldClient 使用在他或她本地计算机的 Cookie 中存贮用户的登录名，主题和某些其他属性，点击此选项。使用此功能给您的用户更多的“自定义”登录体验，但需要在他们的浏览器中，启用了对 cookie 支持。

回复读取确认要求
如果您希望 WorldClient 对包含已读确认请求的进入消息产生回应，请点击此选项。当 WorldClient 用户打开消息时，MDaemon 将会发送一个显示信息已经被收件人看到的提示给发送者。受到消息的 WorldClient 用户将不会看到任何提示关于请求了或者回应了已读确认。
如果您希望 WorldClient 无论消息是否被读，均忽略已读确认请求，请点击此检查框。

WorldClient 连接期间需要 IP 持续
作为一个附加的安全方法，在会话开始时，您可以点击此复选框使 WorldClient 限制每一个用户的通话到用户一开始连接上来的哪个 IP 地址。因此，由于要求持续 IP，则没有任何人可以“偷走”用户的会话。这个配置更为安全，但对于使用动态分配 IP 和改变 IP 地址的代理服务器或者拨号帐号的用户来说，可能会造成一些麻烦。

使用 HTTP 压缩

在 WorldClient 通话中，如果您希望使用 HTTP 压缩，请点击此复选框。

只绑定 WorldClient 的网页服务到这些 IP

如果您希望限制 WorldClient 服务器只到某些 IP 地址，则在此使用逗号分隔，指定这些地址。如果您要对这些区域留空，之后 MDaemon 将会监听所有您为您的主域和次域指定的 IP 地址。

重启 WorldClient（更改端口或 IIS 值改变时需要）

如果您希望重启 WorldClient 服务器，点击此按钮。注意：当改变 WorldClient 的端口设置时，为了可以识别这些设置您必须重启 WorldClient。

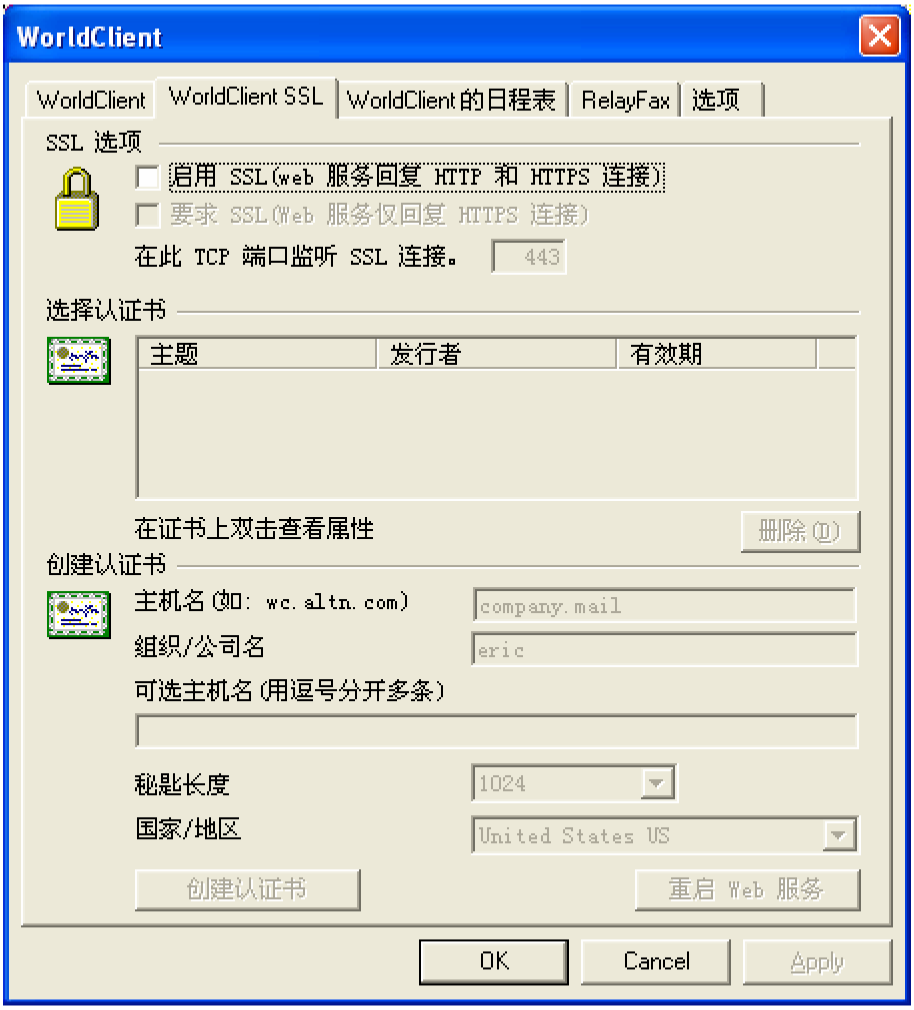
在IIS下，运行WorldClient

WorldClient 配置了一个内建 Web 服务器，因此不需要 IIS 来处理。然而，WorldClient 支持 IIS，所以可以实现 ISAPI DLL 的功能。在 IIS 配置 WorldClient 去工作：

1. 停止 WorldClient。WorldClient 不能同时使用内建的 Web 服务器和 IIS 运行。
2. 在 IIS 中，为\WorldClient\HTML 目录创建网站或虚拟目录。
3. 启用“脚本和可执行”许可，并且设置 WorldClient.dll 作为默认文档。
4. 使用 Windows 资源管理器，对 IWAM_ComputerName 帐号对您的 MDaemon 目录给出完全控制。
5. 如果您有任何使用 NT 域认证的电子邮件帐号，编辑您的本地安全策略给 IWAM——ComputerName“作为操作系统一部分的用户权限。
6. 如果您在 IIS 下运行 WebAdmin，编辑 WorldClient 的 Domains.ini（在\MDaemon\WorldClient\）并在 WebAdmin 中的 URL 的[Default:Settings]设置 WebAdminURL 密匙。
7. 在 MDaemon 中，到设置 – WorldClient – Web 服务，并点击在 IIS 下运行 WorldClient。

注意：
当在 IIS 下运行 WorldClient 时，您将不能在 MDaemon 的界面中，启动或者停止它。您必须使用 IIS 提供的工具才能这么做。

WorldClient SSL



WorldClientWeb 服务器支持 SSL 协议。Netscape 通信公司发展的 SSL 协议，是服务器/客户端网络通信的安全标准方案。它提供了 TCP/IP 连接的服务器认证，数据编码，以及可选的客户端认证。而且，由于在当前主要的浏览器中都内建了 SSL，简单的在您的服务器上安装一个合法的数字认证将会激活连接客户端的 SSL 能力。如果您不能或者没有选择在 IIS 下运行 WorldClient，这种安全方案已经内建在 WorldClient 中。

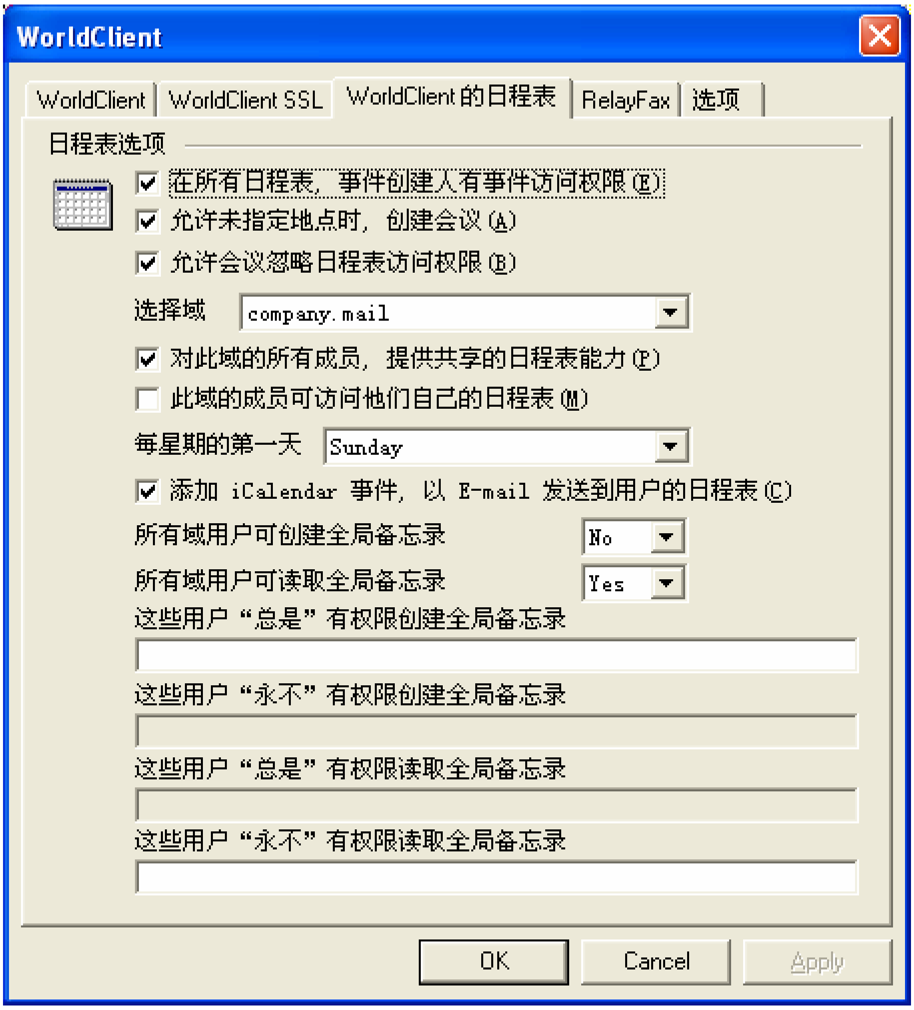
注意：
此对话框只有当时使用内建 Web 服务器时，才会应用到 WorldClient。如果您已经配置了 WorldClient 与 IIS 工作代替它自己的网络服务器，那么将不会使用这些选项 – 必须在 IIS 中设置 SSL 支持。

启用和配置 WorldClient 使用 SSL 的选项在 SSL & 认证对话框上（点击 Ctrl+L 或者安全 – SSL/TLS/认证… - WorldClient SSL）。为了您的方便，这些选项也会在 WorldClient 的对话框上（点击 Ctrl+W 和_WorldClient SSL 或者设置 – WorldClient… – WorldClient SSL）。

此对话框更多信息，请参看 156 页。

SSL & 认证信息，请参看 153 页。

WorldClient的日程表



日程表选项

在所有日程表，事件创建人有事件访问权限

这是全局设置；不能在域上设置。如果您希望事件的创建者可以访问事件和其他人的日历，点击此复选框。如果您希望日历的个人设置可以控制是否允许事件创建者访问事件，请清空此复选框。

允许未指定地点时，创建会议

无论何时创建会议事件，如果您不想要求用户指定会议地点，请点击此检查框。如果您希望在安排会议事件时，强制所有会议都拥有一个指定地点，请清空此检查框。这是全局设置；不能在域上设置。

允许会议忽略日程表访问权限

正常来说，即使您没有与会者日历的写权限，您也可以安排一个会议 – 绕过访问权限。如果您不希望这种情况，清空此复选框。这个选项停用时，在与会者日历上放置一个会议，则需要会议参与者日历的写权限。

选择域

使用下拉列表选择您希望编辑组日程安排和日历设置的域。如果您在此标签上的任何设置做出了更改，您必须在切换一个不同*选择域*设置前*应用*他们。如果您做出更改，然后尝试在没有应用的情况下选择一个域，一个框就将出现，问询您在启用新域前，是否希望保存这些更改。点击 YES 保存更改，或者 NO 解除。

对此域的所有成员，提供共享的日程表能力

如果您希望使被选择域中的 WorldClient 用户可以访问日历系统，点击此选项。如果您清空此选项，则日历系统将会对此域停用，在 WorldClient 导航栏上将不会出现日历链接。

此域的成员可访问他们自己的日程表

如果您希望不阻止域中的用户查看他们的日程表，请点击此选项。

每星期的第一天

从下列表中选择一天。这个选择的日子将会作为此周的第一天出现在域日历上。

添加 ***iCalendar*** *事件，以* ***E-mail*** *发送到用户的日程表*

WorldClient 支持在 Microsoft Outlook 和其他 iCal 适应电子邮件程序中使用的 Internet Calendaring（iCal）。如果您希望在 WorldClient 用户发送的电子邮件中 WorldClient 找到的 iCalendar 事件可以被自动添加到他或她的日历中，请点击此选项。

所有域用户可创建全局备忘录

如果您希望给所有选定的域 WorldClient 用户创建全局备忘录的权限，设置此下拉栏为“YES”。如果您不想，设置为“NO”。您可以通过使用标签下面的文本框指定特殊用户作为此设置的例外，*“这些用户总是/永不有权限创建全局备忘录”*

所有域用户可读取全局备忘录

如果您希望全局备忘录出现在每一个 WorldClient 用户的日历上，设置此下拉框为“YES”。如果不想，设置为“NO”。您可以通过使用标签下面的文本框指定特殊用户作为此设置的例外，*“这些用户总是/永不有权限读取全局备忘录”。*此控制可以在域中设置。

这些用户总是有权限创建全局备忘录

当“所有域用户可创建全局备忘录”设置为“NO”时，使用此控制输入您希望作为例外对待的 WorldClient 用户的电子邮件地址。这些特定的用户将可以创建全局备忘录。使用逗号分隔多个地址。

这些用户永不有权限创建全局备忘录

当“所有域用户可创建全局备忘录”设置为“YES”时，使用此控制输入您希望作为例外对待的 WorldClient 用户的电子邮件地址。这些特定的用户将不可以创建全局备忘录。使用逗号分隔多个地址。

这些用户总是有权限读取全局备忘录

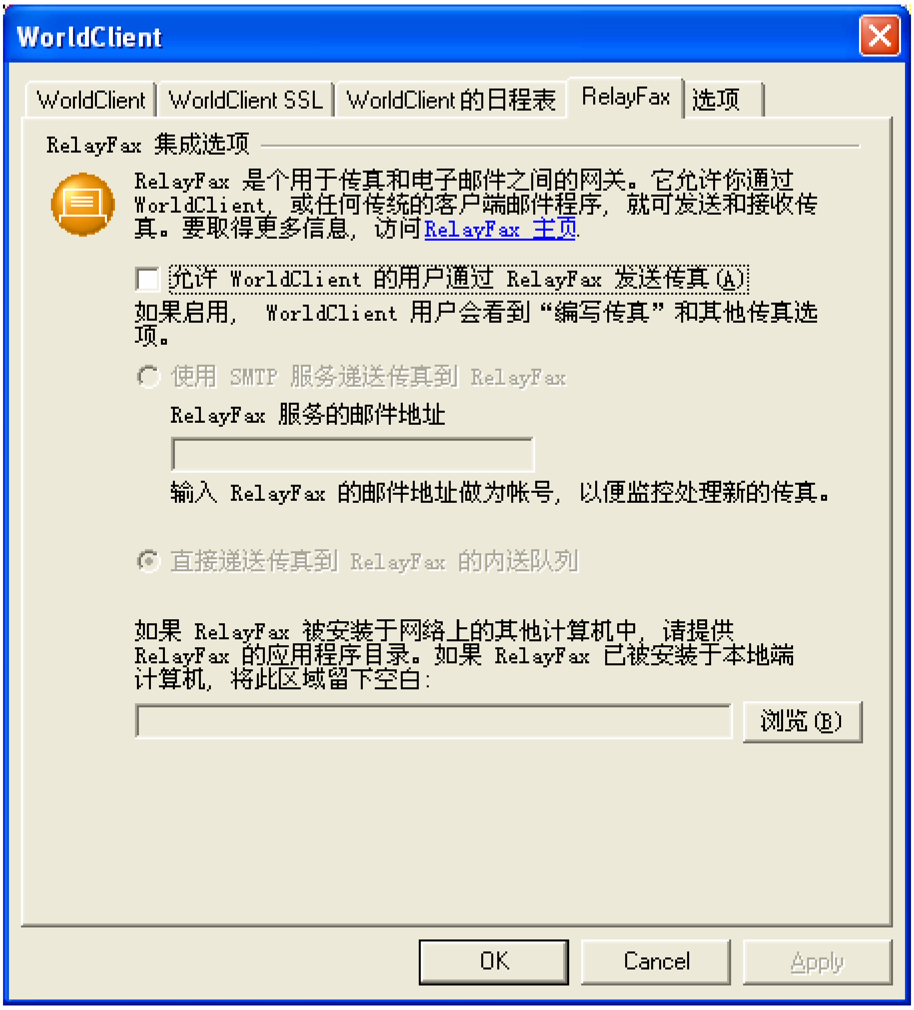
当“所有域用户可读取全局备忘录”设置为“NO”时，使用此控制输入您希望作为例外对待的 WorldClient 用户的电子邮件地址。这些特定的用户将可以读取全局备忘录。使用逗号分隔多个地址。

这些用户永不有权限读取全局备忘录

当“所有域用户可读取全局备忘录”设置为“YES”时，使用此控制输入您希望作为例外对待的 WorldClient 用户的电子邮件地址。这些特定的用户将不可以读取全局备忘录。使用逗号分隔多个地址。

RelayFax

Alt-N Technologies 的 RealyFax 服务是与 WorldClient 无缝整合的电子邮件到传真和传真到电子邮件的网关，以提供给您的用户传真服务。当此功能启用时，WorldClient 用户将会被赋予访问各种功能的权利，这些功能可以通过 WorldClient 页启用他们来编写和发送传真。更多关于 RelayFax 的信息，访问转发 RelayFax 网址 www.relayfax.com。



RelayFax 集成选项

允许 WorldClient 的用户通过 RelayFax 发送传真

点击此选项将 WorldClient 与 RelayFax 整合。当激活时，它会使“编写传真”控制和其他传真相关功能出现在 WorldClient 页上。

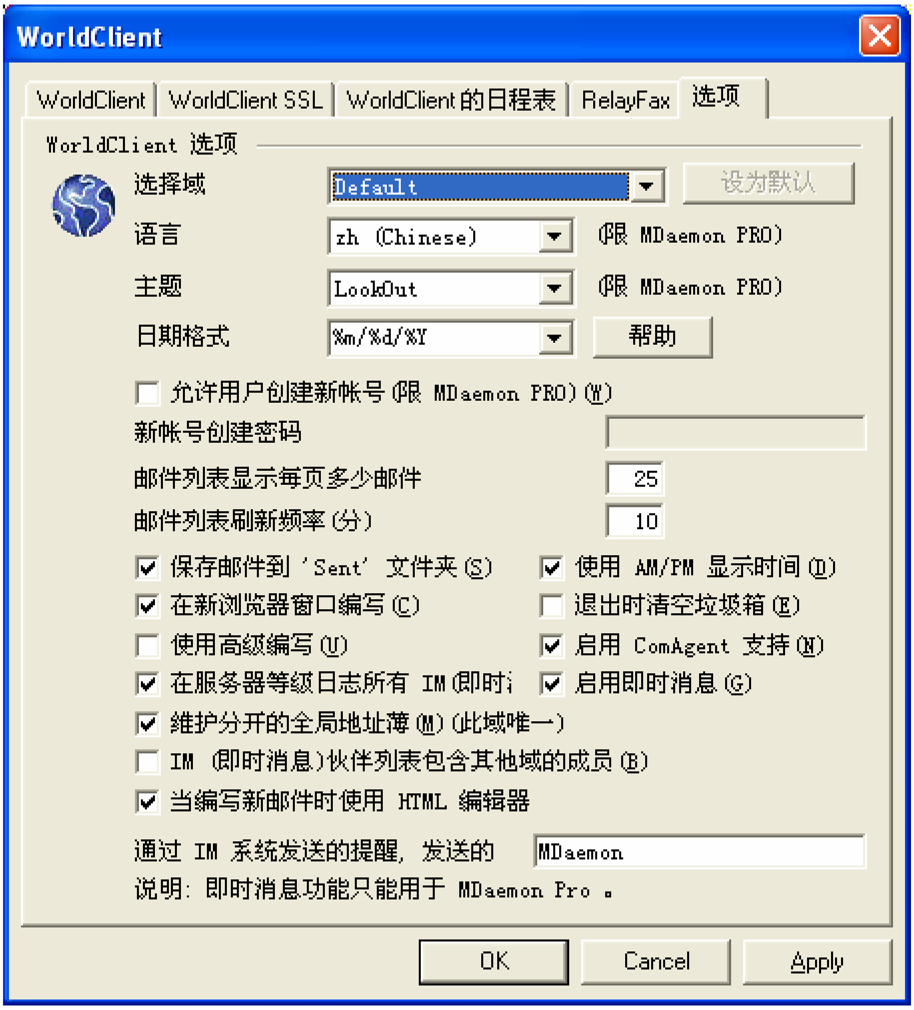
使用 SMTP 服务递送传真到 RelayFax

Relayfax 将会为将被传真的进入邮件监视指定邮箱。点击此选项，MDaemon 将会使用正常的 SMTP 电子邮件发送过程来发送这些邮件到邮箱地址。当 RelayFax 监视其他地方的邮箱而不是您的 LAN 的邮箱时，此选项是很有用的。如果 RelayFax 存在您的 LAN 上，您可能选择让 MDaemon 直接发送消息到 RelayFax 的消息队列，如此可以完全绕过 SMTP 发送处理过程。此方法的更多信息，请参看以下*直接递送传真到 RelayFax 的入站队列*。

RelayFax 服务的邮件地址
指定您希望邮件作为传真发送的电子邮件地址。这个值必须和您配置 RelayFax 监视这些邮件的地址相匹配。

直接递送传真到 RelayFax 的入站队列
如果 RelayFax 存在您的 LAN 中，您应该选择此方法而不是将邮件分发到 SMTP 来发传真。当 MDaemon 收到一个尝试 RelayFax 的邮件时，它将会直接放置又见到 RelayFax 入站队列而不是使用 SMTP 发送。如果 RelayFax 在 MDaemon 运行的同一台机器上，您可以对此文件路径留空。否则，您必须指定 RelayFax 的\app\directory 的网络路径。

选项



在此标签上的设置是域细节。大多数功能和控制会处理客户端级别行为，而不是 WorldClient 服务的全部行为和配置。

WorldClient 选项

选择域

使用下拉列表选择您希望编辑设置的域。如果您希望编辑默认设置，使之设置到默认。默认设置将会对所有您没有特别更改的域设置。如果您在此标签上做出了任何的更改，则您必须在切换不同的*选择域*设置之前应用它们。如果您做出了更改，并且在没有第一次应用它们，尝试选择一个不同的域，在切换新的域前，将出现一个框询问您选择是否希望保存这些更改。点击 YES 保存更改或者 NO 解除它们。

设为默认

此选项重置一个域回复到*默认*设置。使用*选择域*控制来选择一个域，然后点击设为默认回复。

语言（限 MDaemon PRO）

当您的用户第一次登陆到选择的域时，使用下拉列表框来选择 WorldClient 界面中的。用户通过 Worldclient 中**选项 – 个性化设置**的一个选项，可以改变他们的个人语言设置默认语言

主题（限 MDaemon PRO）

当选择了域的用户第一次登陆时，使用下拉列表框为客户端界面指定默认的 WorldClient 主题。使用者可以从 WorldClient 中的**选项 – 个性化设置**页里面自定义主题设置。

日期格式

使用此文本框指定选择的域中的日期将以何种格式显示。点击 Help 按钮显示可以在此文本框中使用的宏代码列表。您可以在此控制中使用以下宏：

%A – 完整的平日名称
%B – 完整的月份名称
%d – 日，月（显示“01-31”）
%m – 月份（显示“01-12”）
%y – 2 位数字年
%Y – 4 位数字年

例如，“%m/%d/%Y”在 WorldClient 中将会显示“12/25/2002”。

注意：
此设置是在每一个域的。个人用户使用他们的帐号不能调整日期格式。

帮助

点击此按钮，显示在以上日期格式中使用的宏定义列表。

允许用户创建新帐号（限 MDaemonPRO）

当一个用户连接到选定的域时，如果您希望“创建帐号”按钮出现在 WorldClient 的登陆界面行，点击此复选框。此功能将使用户通过 WorldClient 可以创建他们自己的 MDaemon 帐号。

提示：
如果您选择允许用户创建他们自己的电子邮件帐号，则您应该细心的查看**新建帐号默认值**设置（289 页）。使用**新建帐号默认值**来指定您将允许用户在他们自己帐号上的控制程度。

新帐号创建密码

如果您希望在登陆界面中，限制那些知道密码的用户创建新帐号，在此输入密码。在“创建帐号”按钮允许他们进行前，用户将必须输入新用户创建密码到在登陆界面上的密码框中。如果没有特定的合理密码情况下，点击*创建帐号*，将会显示一条需要密码的消息。

当用户端显示帐号创建界面时，他们必须指定他们的帐号名（邮箱名），密码，全名，和他们希望在界面中显示的语言。

邮件列表显示每页多少邮件
这是在您的每一个邮件文件夹中，邮件列表的每一页显示的邮件数。如果一个文件夹中包含多余这个数量的邮件，那么将会在列表的上面和下面有几个控制，来允许您移动到其他页去。个人用户可以从 WorldClient 中的**选项 – 个性化设置**页调整这些设置。

邮件列表刷新频率（分）
这是 WorldClient 在自动刷新消息列表前等待的分钟数。个人用户可以从 WorldClient 中的**选项 – 个性化设置**页调整这些设置。

保存邮件到"已发送"文件夹
如果您希望每一个您所发送的邮件的副本都被保存到您邮箱中的已发送文件夹。个人用户可以从 WorldClient 中的**选项 – 编写**调整这些设置。

使用 ***AM/PM*** *显示时间*
当在 WorldClient 中显示此域时，如果您希望使用带 AM/PM 的 12 小时表，请点击此选项。如果您希望为这个域使用 24 小时时钟，清空此复选框。个人用户可以从 WorldClient 中的**选项 – 日历**调整这些设置。

在新浏览器窗口编写
如果您希望打开一个单独的浏览器窗口编写邮件取代简单开启主窗口编写界面，点击此选项。如果您不希望打开单独的窗口，清空此框。个人用户可以从 WorldClient 中的**选项 – 编写**调整这些设置。

退出时清空垃圾箱
当用户从 WorldClient 登出时，此选项可以清空用户的垃圾站。个人用户可以从 WorldClient 中的**选项 – 个人化**页调整这些设置。

使用高级编写
点击此选项使用高级编写而不是域用户默认的打开普通的编写界面。个人用户可以从 WorldClient 中的**选项 – 编写**调整这些设置。

启用 ***ComAgent*** *支持*
此选项可以使 ComAgent 消息功能在被选择的域用户有效。他们可以从 WorldClient 中的**选项 – ComAgent** 上下载它。此下载安装文件将会自动为每一个用户的帐号自定义，使得安全和设置更简便。

启用即时消息
如果您希望域用户激活 ComAgent 及时消息系统，点击此选项。如果您希望即时消息控制不可用，清空此选项。

在服务器等级日志所有 ***IM*** *（即时消息）*
如果您希望所有选定的域即时消息通信量被记录于 InstantMessaging.log 文件中，点击此复选框。（在 MDaemon/LOGS/文件夹下）。

维护分开的全局地址薄（此域唯一）

如果您希望选定的域全局（公共）地址薄对于那个域是唯一的以替代在您的其他域中共享全局联系人，点击此复选框。域全局地址薄文件的名称将会是<DomainName>.xml。对其他域的公共联系人信息将不会列在此列表中，它也不会与其他域共享他的联系人。

IM *（即时消息）伙伴列表包含其他域的成员*

如果您希望您的所有 MDaemon 域的用户都可以添加域好友列表，请点击此选项。如果您希望只有相同的域的用户能够添加好友列表，清空此框。例如，如果您的 MDaemon 为 example.com 和 mycompany.com 管理邮件，则为您的 example.com 用户激活此控制将使他们能够从 2 个域中添加好友到他们的列表。清空它意味着用户可能只能添加其他 example.com 用户。

当编写新邮件时使用 ***HTML*** *编辑器*

如果您希望允许您的用户使用 rich text（HTML）格式编写消息，点击此对话框。

通过 ***IM*** *系统发送的提醒来自*

当一个约会或者会议被安排到用户的 WorldClient 日历中时，可以设置事件在指定时间时发送一个提示给用户。如果对每个用户的域，IM 系统都是激活的，则在用户是用户使用 ComAgent 的前提下，提示将会在即时消息中发送。使用此文本框指定您希望消息中显示“来自”的名称。

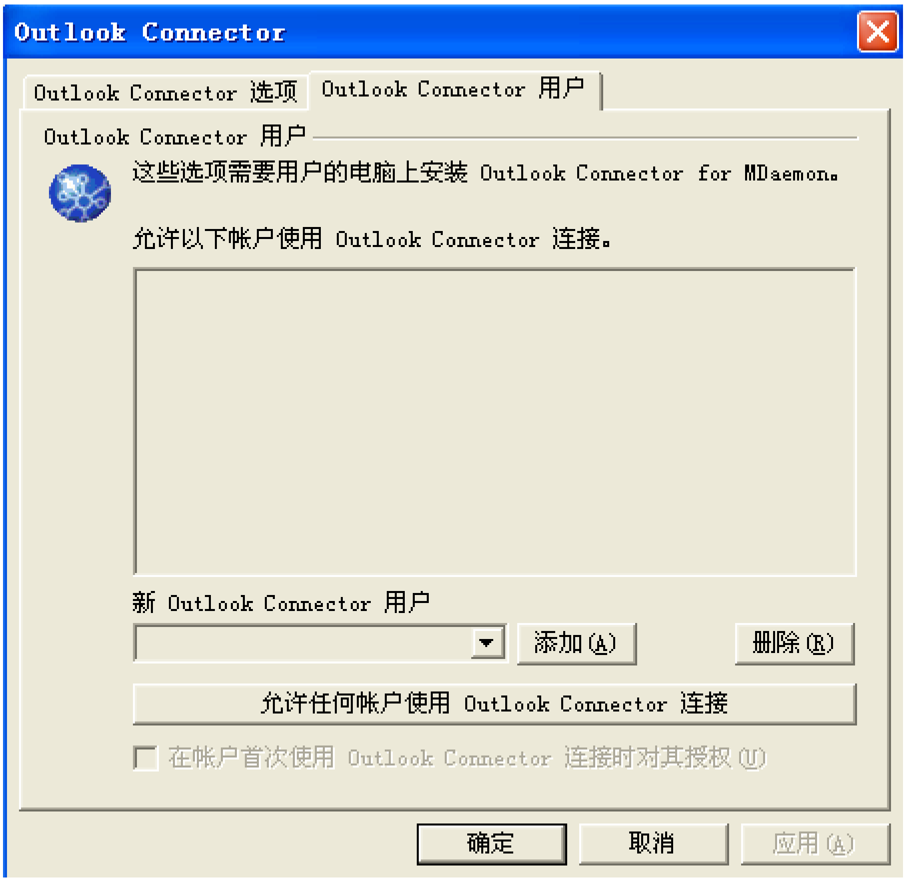
Outlook Connector for MDaemon

MDaemon PRO支持**Outlook Connector for MDaemon**，一个Alt-N Technologies推出的单独授权的产品。Outlook Connector使您能与其他用户共享您的Microsoft Outlook日历，联系人，任务等—这些通常只有在Outlook与Microsoft Exchange Server结合使用时才能实现。Outlook Connector for MDaemon能有效消除您对Exchange的依赖。

当您安装了Outlook Connector for MDaemon，Outlook Connector对话框将可以从设置>Outlook Connector… (或Ctrl+C)打开。这个对话框用于激活和配置Outlook Connector，以及授权特定的账户来使用它。

更多关于Outlook Connector for MDaemon的信息，请访问www.altn.com 。

Outlook Connector 用户



Outlook Connector用户

允许以下账户使用Outlook Connector进行连接

这是被授权通过Outlook Connector来共享他们的Outlook文件夹，日历，联系人等信息的MDaemon用户列表。您能通过如下列出的选项来添加用户到该列表。

新 Outlook Connector 用户

要添加一个新的MDaemon用户到授权的Outlook Connector用户列表，请从这个下拉列表中选择目标用户并点击添加。

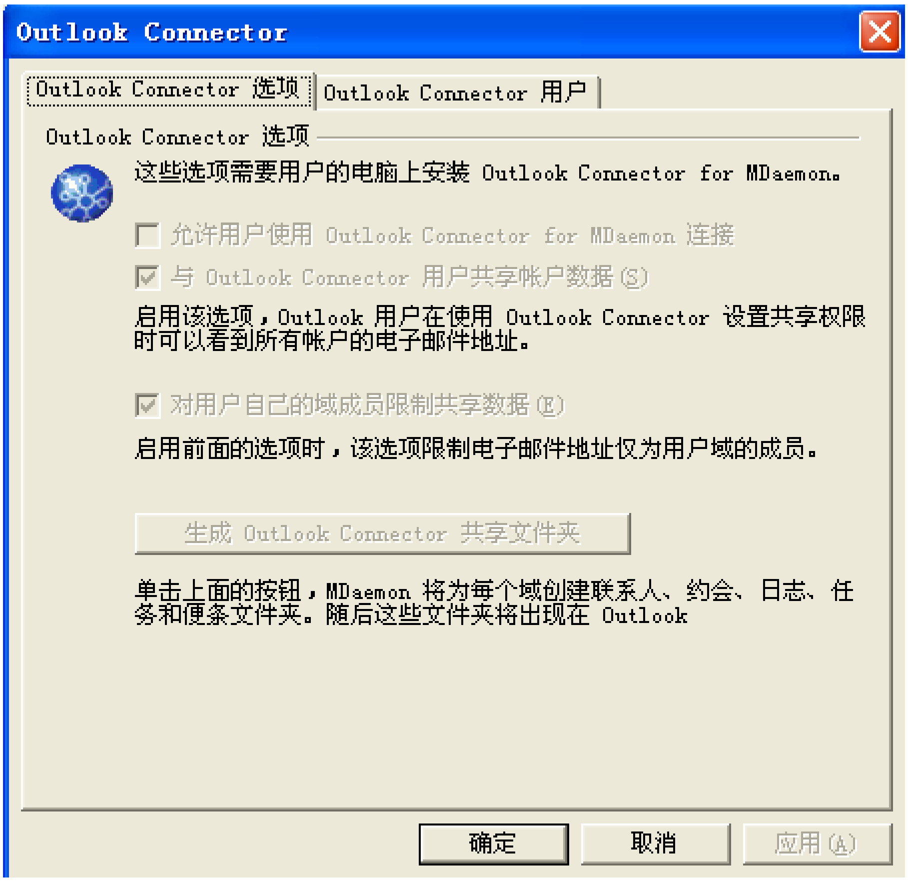
添加
从新的Outlook Connector用户下拉列表中选择了一个用户后，点击这个按钮来添加那个账号到授权的Outlook Connector用户列表中。

删除
要从授权的Outlook Connector用户列表中删除一个账号，在列表中选择目标用户并点击删除。

*允许任何账户使用**Outlook Connector** 连接*
要快速授权所有MDaemon帐号通过Outlook Connector进行连接，点击这个按钮，那么所有的 MDaemon账户都将被添加到…*允许使用Outlook Connector进行连接的账户*列表。

*在账户首次使用 **Outlook Connector** 连接时对其授权*
点击这个复选框，如果您希望每个MDaemon用户都被添加到…*允许使用Outlook Connector进行连接的账户*列表，如果他是第一次尝试使用Outlook Connector进行连接。
注意：如果您激活这个选项，那么您就有效地授权了所有MDaemon账户使用Outlook Connector for MDaemon。账户本身并不会被添加到列表直到用户首次使用以后。

Outlook Connector 选项



允许用户使用 Outlook Connector for MDaemon 连接

点击这个复选框来激活Outlook Connector for MDaemon.。您的用户将不能使用Outlook Connector的功能除非这个选项被选中。

与Outlook Connector用户共享账户数据

点击这个选项如果您想要所有已经被授权通过Outlook Connector进行连接的MDaemon账户在Outlook Connector for MDaemon插件中的*许可列表上*变得可见。当共享Outlook 项目，Outlook Connector用户将从列表中选择那些他们想要授权与其共享的账户。当这个特性被禁用时，Outlook Connector插件的*许可* 列表将变成空白，用户将不得不手动输入email地址。仅有属于被授权通过Outlook Connector进行连接的地址才能共享Outlook项目。如果一个用户输入一个未被授权的邮件地址，那么这个项目将不被共享，除非它以后被授权通过Outlook Connector进行连接。

限制本域中用户共享的数据

这个选项仅当*与Outlook Connector用户共享账号数据* 功能被激活时才可用。点击这个复选框，如果您仅需要那些被授权通过Outlook Connector进行连接的用户和出现在Outlook Connector插件许可列表上属于同一个域的用户—属于不同域的账户将不会被列出，即使它们也被授权通过Outlook Connector进行连接。

生成Outlook Connector共享文件夹

点击这个按钮来为每个域生成一个Outlook Connector文件夹集。它将生成如下文件夹： contact，appointment，journal，task，和note。

附件链接

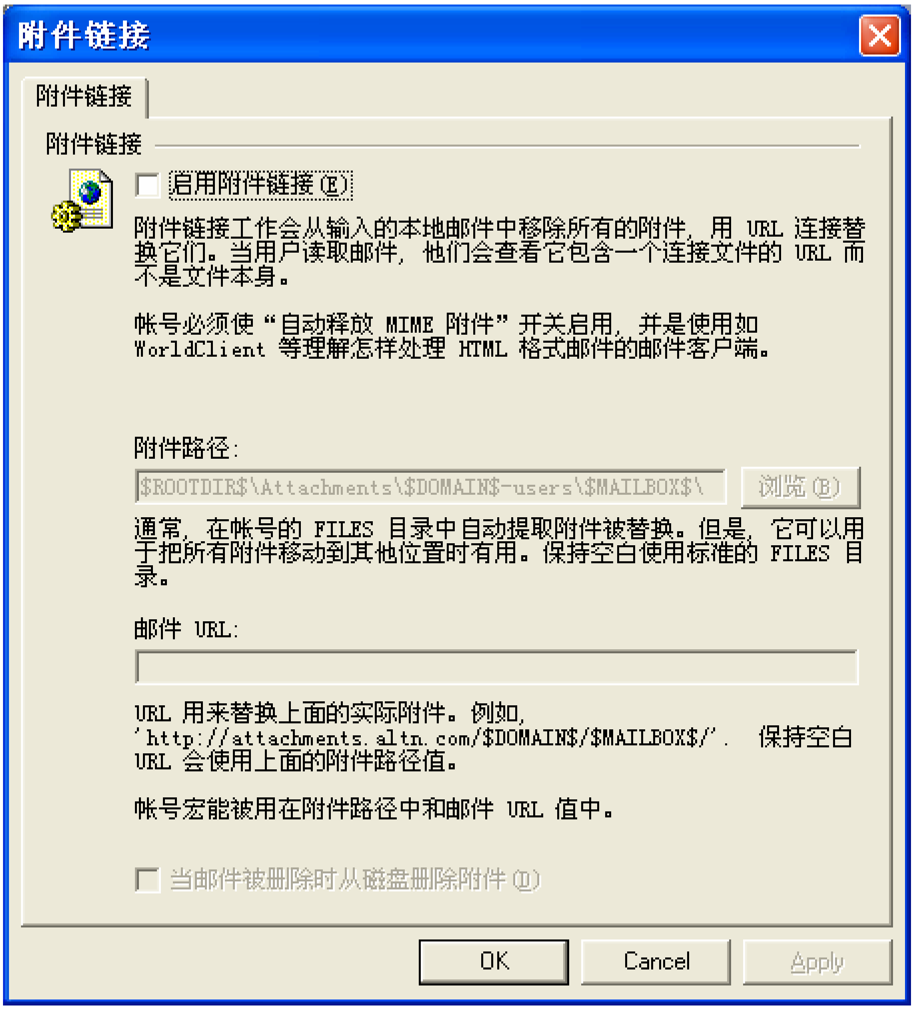
您包含在邮件的 URL 的格式可以通过使用模板和参数设置成动态的。由于您的帐号持有者将会使用此 URL 获得访问他们的文件附件的权利，因此您必须确保制定的存储目录是可以通过 HTML 格式的电子邮件访问的。URL 的格式和参数依赖于您怎么使用它和您希望提供给您的 MDaemon 用户的访问方法。如果您所有的用户都可以从您的本地网络专有的访问他们的电子邮件，那么您应该选择在一个本地可访问而不是通过 Internet 的共享目录来存储附件，此类 URL 格式将根据网络或者 intranet 文件路径。或者，您可能希望对每一个用户附件均可用，则要把他们放到一个公共 html 文件夹，或者通过一个匿名 ftp 访问文件夹。如果您使用 MDaemon 整合的网络服务器，则有一个使得附件对您用户可用的简便方法，那就是将它们放置到 WorldClient 的“HTML”目录的子目录中（通常为“C：\MDaemon\WorldClient\HTML\”）。例如，附件路径可以为，“$ROOTDIR$\WorldClient\HTML\attachment\$DOMAIN$\”，消息 URL 为“http://$DOMAIN:3000/attachment/$DOMAIN$/.”，但是依赖于您网络的安全方案，由于是在公共 html 文件夹中，这些可能使得附件对每一用户可用。您将文件存储到哪里，您的用户怎样得到文件，这些完全由您决定。

警告：
如果您使用 IIS 或者其他一些网络服务器，您应该确认您已经配置了它不允许在您存贮在释放出附件的目录中的脚本或者程序被服务器自动运行。例如来说，IIS 应该不自动运行扩展名为“*.asp”的可执行文件。如果您的服务器自动启动脚本，则一些用户可能发送一个脚本或者附加程序的文件的电子邮件 之后远程启动。这样会表现出一系列的漏洞，可能潜在的给一个怀有恶意的人访问您的服务器。当撰写您的附件路径和消息 URL 时，在思想中要总保持安全意识。

最后，当用户删除 POP，IMAP，或者 WorldClient 邮件时，MDaemon 将会自动地删除所有到此消息的链接附件，以便恢复磁盘空间。

警告：
无论何时在服务器上的附件关联的邮件被删除，MDaemon 都将删除链接附件。由于当邮件被找回后，POP 客户端发送一个指令到邮件服务器以删除每一个邮件是正常的，因此任何通过 POP 客户端接收邮件的用户必须将客户端设置成在服务器上留下邮件。如果通过 POP 客户端收到邮件不能在服务器上设置成留下邮件，则在收到每一个消息后，附件将立即被删除。因此，意图给用户的附件将不可补救的丢失，而且邮件中的 URL 将会指向一个已经不存在的文件。事实上，所有 POP 邮件客户端都支持在服务器上留下消息这个选项。 如果您希望阻止释放的附件被删除，则您可以关闭这个选项，“当消息被删除时，从磁盘上删除附件”。通过关闭这个选项，

无论原本附件所附属的邮件状态如何，也无论使用何种协议收集有消息，附件都不会被删除。



附件链接

启用附件链接

点击此复选框，为所有配置从邮件中释放附件的账户启用附件链接。"*自动启用释放 MIME 编码附件*"选项位于账户编辑器的邮箱标签上。当您点击*启用附件*链接选项时，您将被问询是否您希望为所有 MDaemon 帐号启用自动附件释放。如果您选择"否"，则附件链接将会启用，但是您必须为每一个您希望使用附件释放，手动激活它。

附件路径

使用此文本框制定您希望存储释放文件附件的目录。您可以使用模板和消息宏来使得路径成为动态的。

邮件 URL

这个基础 URL 将会插入邮件中。例如，如果文件名为"myfile.gif"从一个邮件中释放，而 Message URL 将被设置成"http://example.com/attcahments/"，则插入

到消息的 URL 将会是“http://example.com/attcahments/myfile.gif。”

当邮件被删除时从磁盘删除附件

无论何时附件链接的消息被删除，如果您希望释放的附件从服务器上被删除，点击此选项。在启用前，请慎重考虑。如果它启用了，并且一个用户通过没有设置成在服务器上留下消息的 POP 客户端收集他的邮件，那么所有他释放的附件将会不可挽回的丢失。如果此选项没有开始，则不会有附件丢失，但是您大量的硬盘空间最终将被过期的文件占满，除非他们原本的收件人不再想要或者需要。

第七章

MDaemon® 中文版

LDaemon/全局地址薄

使用LDAP，支持全局地址薄

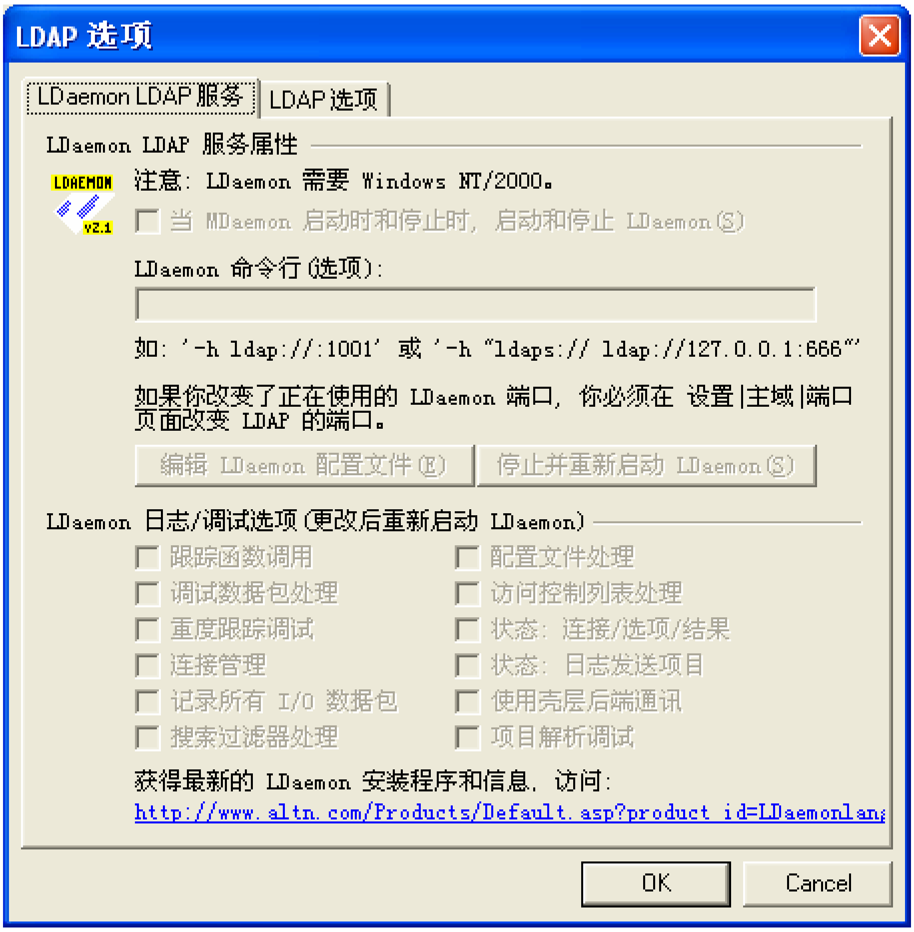
MDaemon 支持轻量级目录访问协议（LDAP）功能。点击设置 – LDaemon/LDAP…打开 LDAP 选项对话框来配置 MDaemon 保持您 LDAP 服务器在所有用户账户上的更新 – MDaemon 可以通过与 LDaemon 的通信，维护一个精确的连续的对用户 LDAP 数据库的更新。这使得用户支持 LDAP 的邮件客户端可以共享全局地址薄以及您包含的其他联系人成为可能。

您也可以使用 LDAP 服务器作为 MDaemon 用户的数据库，而不是它的本地 USERLIST.DAT 系统或者一个 ODBC 数据库。如果您有多个 MDaemon 服务器在不同的位置，但希望他们共享一个单独用户的数据库，您可能想使用这种维护您的用户信息的方法。每一个 MDaemon 服务器都将被配置成访问相同 LDAP 服务器，以便于共享用户信息而不是本地存储它。

最后，您也可以使用此对话框来管理 Alt-N 的 LDaemon LDAP 服务器。您可以获得这个基于 LDAPv3 标准的服务器。免费从 www.altn.com 获得

更多使用您的 LDAP 服务器作为账户数据库的信息，请参看 LDAP 选项 – 109 页和帐号数据库选项 – 281 页。

LDaemon



这个标签用来控制 Alt-N Technologies 的 LDaemon LDAP 服务。注意：这些控制在只有在安装了 Ldaemon 才可用。LDaemon 可以从 ftp://ftp.altn.com/LDaemon/免费下载。

LDaemon LDAP 服务属性

当 MDaemon 启动时和停止时，启动和停止 LDaemon。

当 MDaemon 启动或者停止时，如果您希望启动 Mdaemon，LDAP 服务器也启动或者停止，请点击此复选框。

LDaemon 命令行（选项）

如果您希望使用一些 LDaemon 开启的命令行，您可以通过在这个控制中输入命令行来实现。

编辑 LDaemon 配置文件

点击此按钮为在默认的文本编辑器中打开 LDaemon 配置文件

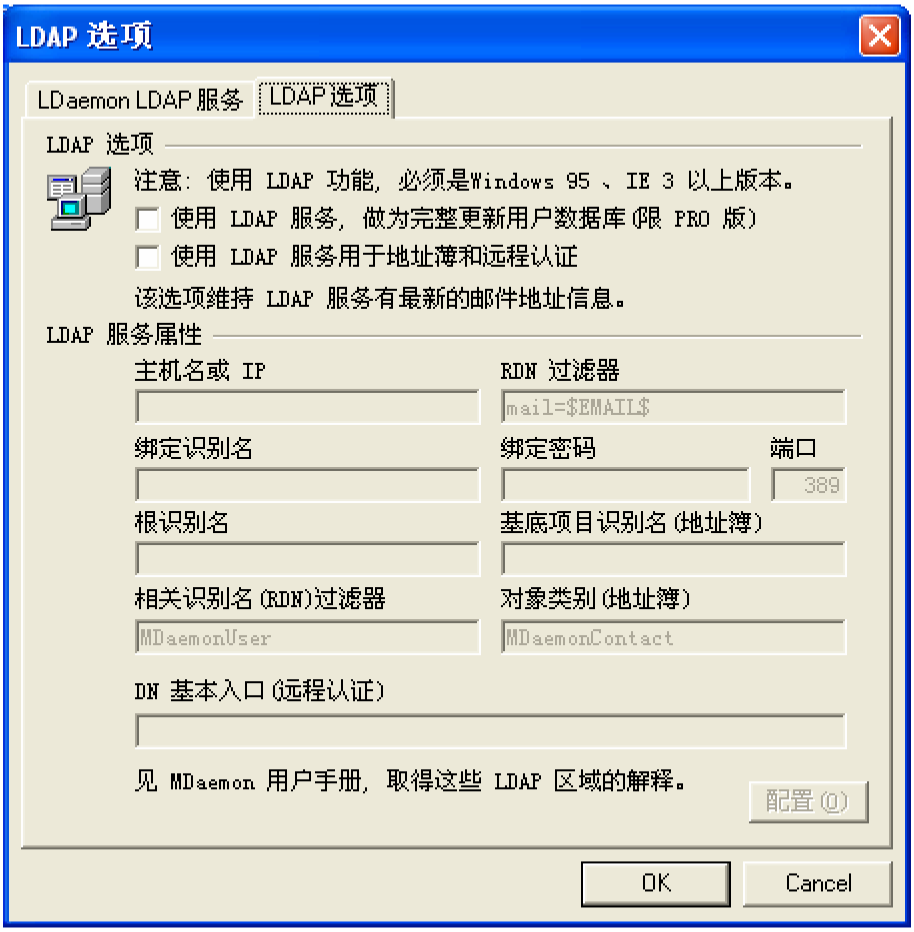
停止并重新启动 LDaemon

在对 LDaemon 做出任何更改后，点击此按钮停止并重启 LDAP 服务器，以便您的更改可以生效。

LDaemon 日志/调试选项

这部分包括各种对 LDaemon 的日志/调试选项。在做出任何针对此这些选项的更改后，您必须重启 LDaemon 才能使新设置生效。

LDAP选项



LDAP 选项

<u>在 LDAP 中存储用户帐号信息（限 PRO 版）</u>

如果您希望 MDaemon 使用您的 LDaemon 服务器作为 MDaemon 用户数据库而不是 ODBC 或者它的本地 USERLIST.DAT 系统，点击此选项。如果您有多个 MDaemon 服务器在不同的位置，但希望他们共享一个单独用户的数据库，您可能想使用这种维护您的用户信息的方法。每一个 MDaemon 服务器都将被配置成链接相同 LDAP 服务器，以便于共享用户信息而不是本地存储它。

<u>使用 LDAP 服务用于地址簿和远程认证</u>

如果您使用 ODBC 或者默认的 USERLIST.DAT 方法来维护您的帐号数据库而不是 LDAP 服务器方式，您仍然可以使用 LDAP 服务器与您的用户名，电子邮件地址，以及别名保持更新。因此，您可以使 LDAP 服务器为包含支持 LDAP 地址薄的电子邮件客户端的用户使用全局地址薄保持更新。

这将维持您的邮箱，别名，及可以查询远程地址信息认证的远程备份服务器的邮件列表。更多信息，参看下面的 *DN 基本条目（远程认证）*。

LDAP 服务器属性

主机名或 IP

在此输入您的 LDAP 服务器的主机名或者 IP 地址。

RDN 过滤器

此控制用来为每一个用户的 LDAP 条目生成 RDN。相关区别名（RDN）在每一个登陆区别名（DN）的最左边。为了所有的对等条目，RDN 必须是独一无二的，因此我们建议使用每一个用户的电子邮件地址作为他们的 RDN，以免可能的冲突。当用户的 LDAP 创建条目时，使用$EMAIL$宏作为在控制中的特征值（例如 mail=$EMAIL$）将会使它通过用户的电子邮件地址被替换。用户的 DN 将会包括 RDN plus 和基础条目 DN。

绑定识别名

输入您赋予的对您的 LDAP 服务器的管理员权限的登陆 DN，可以使 MDaemon 添加并调整您的 MDaemon 用户条目。这是在绑定处理中用来认证的 DN。

绑定密码

此密码将会通过您的 LDAP 服务器单独的为认证绑定密码。

端口

制定您的 LDAP 服务器监视的端口。当发送账户信息到它时，MDaemon 将会使用这些端口。

根识别名

当存储账户信息到一个 LDAP 数据库地址薄时，输入将会在您的 MDaemon 用户地址薄条目中使用的基础登陆（DN 根）。基础条目 DN 是由 RDN（见上面的 RDN 过滤器）组合每一个用户的区别名（DN）构成的

对象类型（地址薄）

指定每一个 MDaemon 用户数据库登陆必须属于的目标级别。每一个输入都将包含 objectclass=功能作为它的值。

DN 基本条目（远程认证）

一个域网关和备份服务器的常见问题时他们通常没有检测一封来信的收件人是否合法的方案。例如，如果一封 frank@example.com 的邮件来自 example.com 的备份服务器，则备份服务器没有方法知道这是否是“frank”在 example.com 的一个真实的邮箱，别名或者邮件列表。因此备份服务器无选择接受所有邮件。MDaemon 包括检验这些地方和解决此问题的方案。通过指定一个为所有邮箱，别名和邮件列表所使用的基础登陆 DN，您的 LDAP 服务器可以保持所有这些信息的更新。之后，每次消息到达您的域，备份服务器会简单得问询 LDAP 服务器并且检验发件人的地址是否合法。如果它不是，则信息将被拒绝。

注意：
尽管可能使用任意的 LDAP 服务器，但是我们推荐使用最新产品的 Alt-N Technologies 的 LDAP 服务器，LDaemon2.1，这是因为它的整合功能和轻松的设置。您可以从 www.altn.com 上面免费获得 LDaemon。

配置

点击此按钮在文本编辑器中，打开 LDAP.dat 配置文件。这将被关联到每一个

MDaemon 帐号区域的指定 LDAP 属性名称是非常有用的。

第八章

MDaemon ® 中文版

共享文件夹/邮件队列

创建额外的邮件队列，配置并使用共享IMAP文件夹

MDaemon 支持共享 IMAP 文件夹 – 公共和用户文件夹都可以共享。公共文件夹是不属于任何特殊帐号的额外文件夹，但是可以对多 IMAP 用户可用。用户文件夹是属于个人 MDaemon 帐号的 IMAP 文件夹。不要搞混公共 FTP 或者 html 文件夹，MDaemon 共享 IMAP 文件夹，是否公共或者用户的，否则可能无法让他人访问。每一个共享文件夹必须拥有一个与之关联的 MDaemon 用户列表，而且只有访问列表上的用户可以通过 WorldClient 或者 IMAP 电子邮件客户端访问它。

当 IMAP 用户访问他们个人文件夹列表时，共享公共文件以及给定访问权限的共享用户文件夹将会显示出来。 在这方面，某些邮件文件夹可以被多用户共享，但是仍需要每个用户的个人登陆信息。而且，拥有一个文件夹的访问权并不意味着对此文件夹拥有全部的读/写或者管理员权限。特别访问权可以授予个人用户，因此对每一个用户，允许您设置不同的访问级别。例如，您可能允许某些用户删除消息，同时限制某些用户进行此操作。

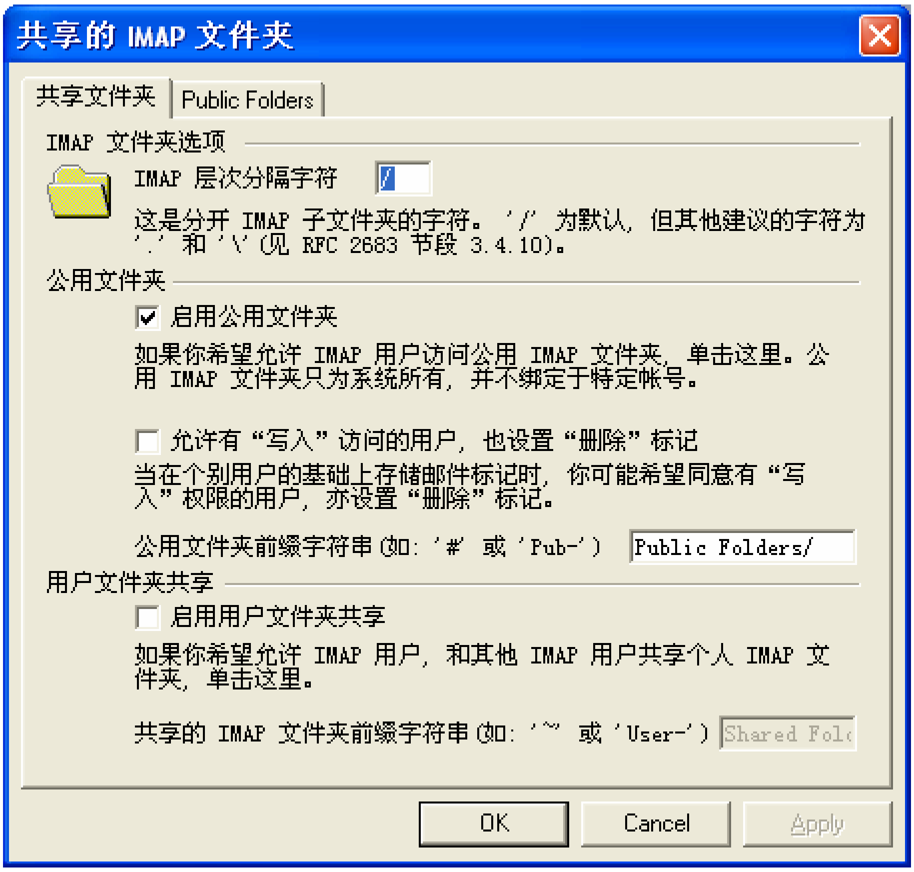
一旦创建了公共或者个人 IMAP 文件夹，您就可以使用内容过滤器来设定规则使哪些文件移动到这个文件夹。例如，这对使得在 TO：邮件头中，包含 support@mydomain.com 邮件移动到 Support 公共文件夹这一规则是非常有用的。内容过滤器的操作“移动邮件到公共文件夹…”和“复制消息到文件夹…”使之成为可能。对共享用户文件夹，您可以使用个人 IMAP 邮件规则来使来特定邮件到此文件夹。另外，使用内容过滤器和 IMAP 邮件规则，您可以将一个指定用户关联到一个共享文件夹，使得目标为“提交地址”的邮件自动被发送到共享文件夹。但是，只有那些被授权对文件夹有“投递”权限的用户才将能发送到这些地址。

为了更多的便利，邮件列表编辑器也包含一个公共文件夹标签可以为您配置公共文件夹。如果您启用此功能，则每个列表邮件的拷贝将会放置到指定公共文件夹中。所有公共文件夹都将存储到 MDaemon 目录层级中的\Public\Folders\目录中。

共享IMAP文件夹

点击 MDaemon 菜单栏上的设置 – 共享的 IMAP 文件夹…可以到达共享 IMAP 文件夹。

共享文件夹



IMAP 文件夹选项

IMAP 层次分隔字符

当使用一个文件夹名称时，输入您希望分隔下级文件夹的字符。例如，如果这个字符被设置成“/”，并且您在公共文件夹标签上有被称作“My Folder”的公共文件夹，则在下级文件夹中创建，您可以命名您的新文件夹为“My Folder/My Subfolder”。当 IMAP 用户连接到 MDaemon 时，“My Subfolder”将会“My Folder”的下级文件夹列在他们的文件夹中。

注意: 尽管下级文件夹将作为您电子邮件客户端 IMAP 文件夹列表中的下级文件夹中显示出来，但是它不是真正在服务器上的下级文件夹。它是包含通过分隔符分开的文件夹和下级文件夹的父系文件夹。

公用文件夹

启用公用文件夹

如果您希望允许 IMAP 用户获得公共文件夹的访问权，点击此开关。在公共文件夹标签上的每一个文件夹下，可以指定能够访问它们的用户以及授予的访问权限。如果您想从那里隐藏公共文件夹，清除此复选框。

允许有‘写入’访问的用户，也设置‘删除’标记

‘写’权限意味着用户可以‘标记’消息作为已读，未读或者其他。如果您希望那些您赋予‘写’权限的用户也可以标记消息为‘删除’，点击此复选框。

*公用文件夹前缀字符串（如：**‘#’**或**‘pub-’**）*

公共文件夹可以用最多 20 个字符作为前缀，比如‘#’或者‘Public-’。这可以帮助用户方便的区分来自他们电子邮件客户端软件中的个人文件夹的公共信息。使用此文本框可以指定您希望用来分隔公共文件夹的一系列字符。

用户文件夹共享

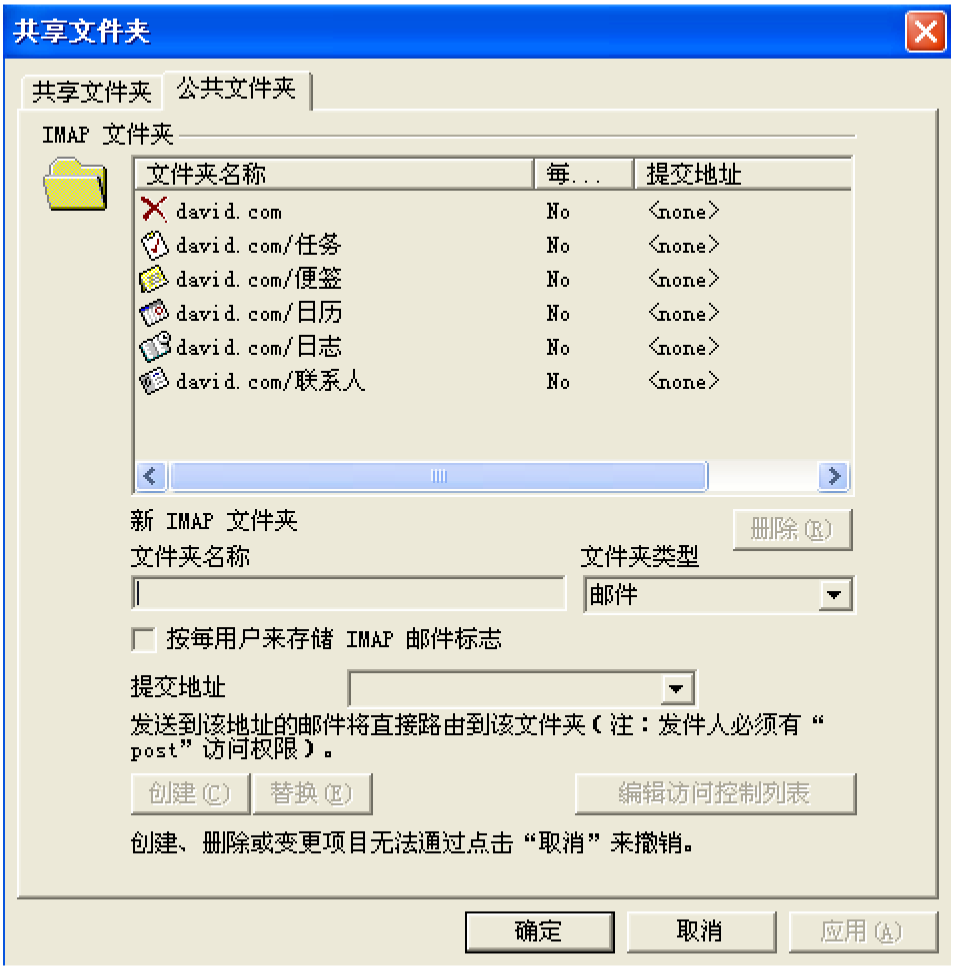
启用用户文件夹共享

如果您希望允许 IMAP 用户共享他们 IMAP 文件夹，点击此开关。在每一个文件夹下，可以在帐号编辑器的共享文件夹标签上指定能够访问它们的用户以及授予的访问权限（MDaemon 的菜单栏上的帐号 – 帐号管理器… – 用户帐号）。如果您希望阻止用户共享访问他们的文件夹，清除此复选框。

*共享的 **IMAP** 文件夹前缀字符串（如：**’~’**或**‘User-’**）*

公共文件夹可以用最多 20 个字符作为前缀，比如’~’或者‘User-’。这可以帮助用户方便的区分来自他们电子邮件客户端软件中的个人文件夹的公共信息。使用此文本框可以指定您希望用来分隔公共文件夹的一系列字符。

公共文件夹



IMAP 文件夹

在此区域显示的是每一个您创建的公共文件夹，每个用户标记设置，以及每一个与相关联的提交地址。当 MDaemon 第一次安装后，这个区域将是空的，直到您使用文件夹名称添加一个文件夹到其中。在此列表中的下级文件夹将有通过共享文件夹标签上指定的分隔符所分离的文件夹和下级文件夹名称。

移除

从列表中移除一个公共 IMAP 文件夹，选择希望的文件夹然后点击移除按钮。

新 IMAP 文件夹

文件夹名

添加一个新的文件夹到列表中，在此中为其指定一个名字，设置每个用户的标记和提交地址控制，然后点击‘创建’。如果您希望新的文件夹作为此列表中的一个文件夹的下级文件夹，使用父系文件夹名称前缀新建文件夹，并且使用在共享文件夹标签上指定的分隔符。例如，如果分隔符是‘/’并且父系文件夹是“My Folder”，则新下级文件夹名将为“My Folder/My New Folder”。如果您不想对下级文件夹作此操作，则将不会使用前缀命名新建文件夹“My New Folder”。

基于用户标记，存储 ***IMAP*** *邮件标记*

如果您希望文件夹的邮件标记（已读，未读，回复到，转发，及其他）将会以每个用户为基础而不是全部性的，那么请点击此复选框。每一个用户可以查看在共享文件夹中消息状态，这些状态可以通过他们个人交互操作显示出来。

如果关闭此控制，则所有用户都将看到相同的状态。因此，一旦任何用户读了一个邮件，则所有用户都将看到它的状态为‘已读’。

提交地址

使用此下拉列表将一个共享文件夹与特殊用户相关联，可以使目标为‘提交地址’的邮件自动的路由到共享文件夹中。但是，只有哪些授予了‘投递’权限到文件夹的用户才能发送到那些地址。

创建

在指定一个文件夹的名称和其他设置后，点击此按钮添加文件夹到此列表。

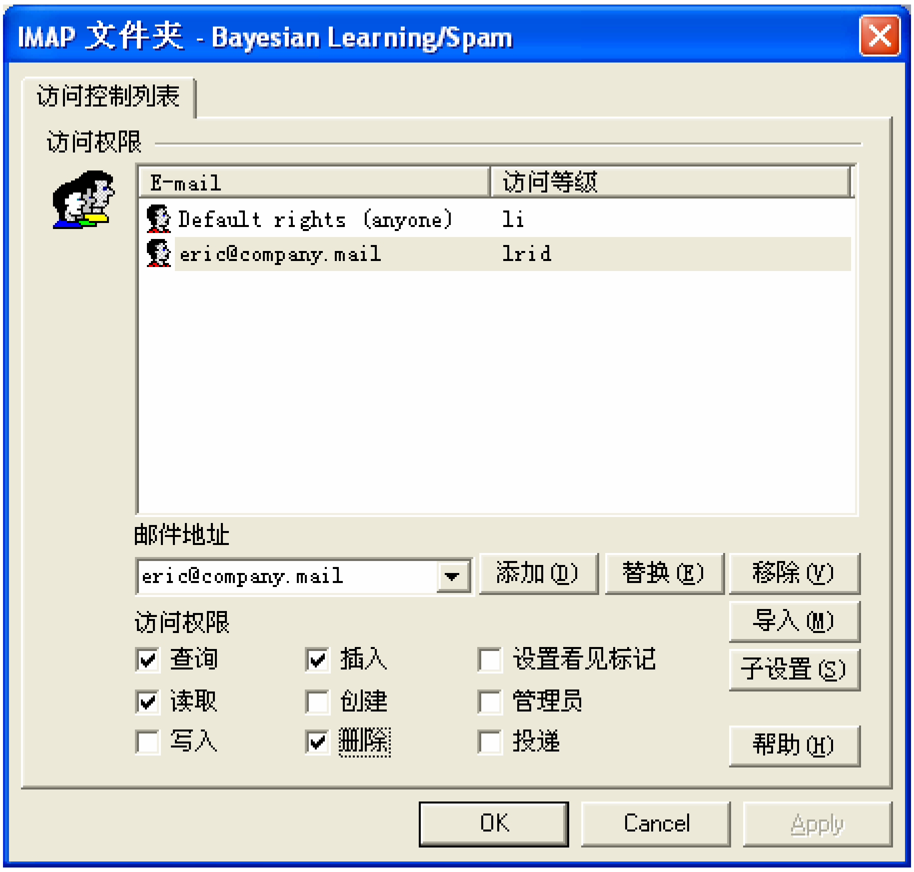
替换

如果您希望编辑公共文件夹条目之一，点击条目，将希望的更改放到*文件夹名称*或者其他设置中，然后点击*替换*。

编辑访问控制列表

选择一个文件夹，然后点击此按钮打开那个文件夹的访问控制列表对话框。使用访问控制列表对话框可以为每一个用户指定能够访问文件夹和权限的用户。

访问控制列表



访问权限

这个区域是用来指定您希望授予共享文件夹权限的 MDaemon 用户帐号，以及为每一个人设置访问权限。您可以从共享 IMAP 文件夹对话框的公共文件夹标签中，到达此对话框（点击设置 – 共享的 IMAP 文件夹… – Public Folders）。双击需要的文件夹，或者点击文件夹，之后点击*编辑访问控制列表*，为此文件夹打开访问控制对话框。每一个条目列出帐号的邮件地址和关于您授权给用户每一个访问权的访问级别的一个字母的缩写。

邮件地址

从下拉列表中，选择您希望授予访问共享文件夹权限的 MDaemon 帐号。

添加

在从列表中选择一个电子邮件地址，以及您希望授予用户的访问权限后，点击*添加*来添加帐号到列表中。

替换

为了调整一个已经存在的访问权条目，选择条目，将希望的更改添加到访问权中，然后点击*替换*。

移除

从访问权列表中移除一个条目，选择需要的条目然后点击*移除*。

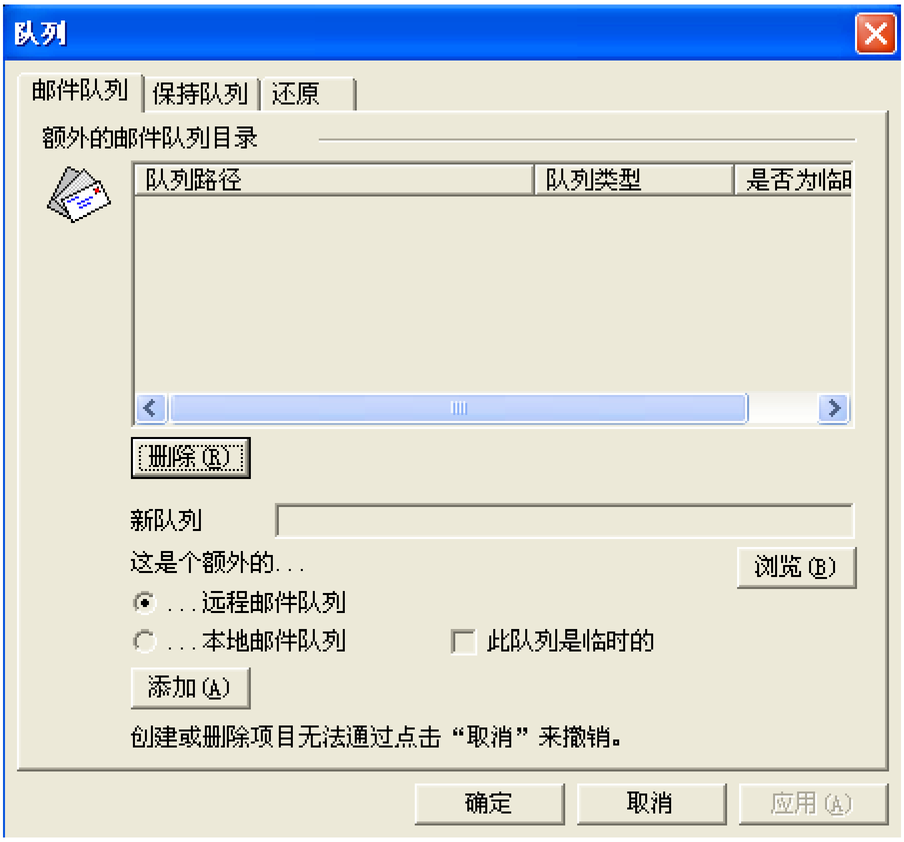
导入
利用导入功能，您可以添加一个已存在邮件列表的成员到访问权用户的列表中。选择您希望授予用户的访问权，点击导入，然后双击需要的列表。所有列表中的用户都将被添加到您设置的访问权列表中。

访问权限
通过特定区域里面需要的选项，选择您希望授予个人用户的权力，然后为新的条目点击*添加*，或者替换已存在条目。
您可以授权以下访问权：
查询（l） - 用户在他们个人的 IMAP 文件夹列表中可以看到此文件夹
读取（r） - 用户可以打开此文件夹和查看它的内容。
写入（w） - 用户可以改变此文件夹中邮件的标记。
插入（i） - 用户可以添加或者复制邮件到此文件夹中。
创建（c） - 用户可以在此文件夹中创建下级文件夹。
删除（d） - 用户可以从此文件夹中删除邮件。
设置看见标记（s） - 用户可以改变此文件夹中邮件的已读/未读状态。
管理员（a） - 用户可以对文件夹进行 ACL 管理。
投递（p） - 用户可以直接发送邮件到此文件夹中（如果文件夹允许）。

帮助
点击帮助显示访问权列表和他们的定义

注意：
访问权可以通过 MDaemon 对访问控制列表（ACL）的支持进行控制。ACL 是 Internet 消息访问协议（IMAP4）的扩展，它可以使您为您的每一个 IMAP 消息文件夹创建一个访问列表成为可能，因此授予在您的邮件服务器上也有帐号的其他用户对您的文件夹的访问权。 在 RFC2086 中有完整的讨论，可以在以下地址中查看到： http://www.rfc-editor.org/rfc/rfc2086.txt

邮件队列



使用队列对话框（点击在菜单栏中的队列 – 队列）创建自定义本地和远程邮件队列。自定义队列支持可以使您让 MDaemon 监视几个来自发送邮件的位置成为可能。在邮件队列标签上，您可以创建新的队列，指定他们作为本地或者远程，以及制定是否新的队列为临时。临时队列将会使用在下一个邮件处理间隔中，之后从邮件队列列表中删除。您可以使用内容过滤器（225 页）来使邮件自动放入到您的自定义邮件队列中的之一。

附加的邮件队列目录

这个区域显示每一个自定义队列的条目，列表是否为本地或者远程，以及是否临时或者固定。

移除

如果您希望从列表中移除一个队列时，选择它的条目，然后点击*移除*按钮。

新建队列

使用此文本区域，列出您希望作为一个邮件队列制定的文件夹路径。

这个是附加的...

...远程邮件队列

如果您希望自定义邮件队列用于远程邮件，选择此选项。

...本地邮件队列

如果您希望自定义邮件队列用于本地邮件，选择此选项。

这个队列是临时的
如果您希望队列为临时，点击此复选框。它将会在下一个邮件处理间隔期间被使用，然后从列表中移除。

添加
在您列出新的队列的路径并且制定它的其它参数后，点击*添加*按钮来添加它到自定义队列列表中。

保持队列

Holding队列(通过点击菜单栏上队列>队列…>保持队列进行配置) 可以被用于接收那些在防病毒，反垃圾邮件或内容过滤进程中可能会导致软件异常的邮件。如果在处理一个邮件时发生某个软件错误，这个邮件将被转移到holding队列中并不被发送。被放置到holding队列中的邮件将留在其中直到管理员采取措施来将它们移走。在主用户界面上有一个*处理holding队列* 按钮，在队列菜单上也有一个同样的选项(点击队列>处理保持队列或按Ctrl+F11)。您也能通过在主界面上右击保持队列然后从右击菜单中选择“重新排队”来处理这些邮件。处理保持队列将移动其所有的邮件到远程或本地队列用于正常的邮件处理。如果引起邮件发生错误的原因依然存在，那么在发生错误时邮件将被重新放回holding队列中。如果您想尝试发送holding队列中的邮件而忽略任何可能发生的错误，那么您可以通过在主界面上右击保持队列并从右击菜单中选择“释放”来实现。当从保持队列中释放邮件时，将会打开一个确认框来提醒您这些邮件可能包含病毒否则它们不会在防病毒，反垃圾邮件或内容过滤进程中被排除。

保持队列
激活和使用保持队列
点击这个复选框来激活holding队列。一旦错误发生，在防病毒或内容过滤进程中被排除的邮件将被移动到这个队列中。

在垃圾邮件过滤器遭遇错误时使用保持队列
点击这个选项，如果您还想将在垃圾邮件过滤进程中引起错误的邮件移动到保持队列中。

发送队列内容概要到如下地址
如果您想定期发送holding队列中信息的概要到一个或多个email地址，那么请点击这个选项并在所提供的文本内列出地址。当列出多个地址时，用逗号分隔。通知邮件在MDaemon启动时被发送，一个邮件首次被放置到保持队列中，并在*每隔XX分钟发送概要*选项下指定的时间间隔被发送。

注意
如果一个通知邮件引起软件错误，那么它可能不会被发送给远程收件人。它将仍

然被发送到本地收件人。

发送概要到内容过滤器管理员
点击这个选项，如果您想要一个额外的通知邮件副本被发送给内容过滤器管理员。管理员在内容过滤器的Admins/Attachments标签中指定。.

每隔XX分钟发送概要
使用这个选项来指定MDaemon发送holding队列通知邮件到每个指定的地址或内容过滤器管理员的时间间隔。

还原

队列位置还原
重置队列位置到安装默认值
默认状态下，一次全新的MDaemon安装过程将存储邮件队列例如远程，本地，未处理等等到`\MDaemon\Queues\`子目录下。先前版本的MDaemon是存储在其它地方。如果您的安装使用原先的文件夹地址，而且您想移动队列到这个更有组织的结构，那么请点击这个按钮，所有它们包含的队列和文件以及邮件都将被移动。点击这个按钮之后，您将需要重新启动MDaemon来让改变生效。

第九章

MDaemon ® 中文版

安全功能

MDaemon的安全和屏蔽功能

MDaemon 配备了一套扩展的安全功能和控制。点击 MDaemon 菜单栏上的安全到达以下安全功能。

安全特性

- **AntiVirus –** MDaemon 反病毒可以通过为 MDaemon 用户提供的最高级别的整合保护帮助您阻止电子邮件带来的计算机病毒。它可以捉住，隔离，修复，并且/或者移除发现包含病毒的电子邮件消息。更多 MDaemon 反病毒信息，请参看 239 页。
- **内容过滤器 –** 一个更为多用的内容过滤器系统使您自定义基于进来与外发的电子邮件消息内容成为可能。您可以插入和删除消息邮件头，添加消息注角，移除附件，路由拷贝到其他用户，使得一个即时消息发送到某人，运行其它程序，以及更多。更多的内容过滤信息请参看 225 页。
- **垃圾邮件封锁器 –** 允许您指定一个 ORDB 和 MAPS RBL 类型的主机，在每一次某些用户试图发送消息到您的服务器时，将会去这些主机核查。如果连接的 IP 已经被这些主机中的任何一个列入黑名单，邮件将会被拒绝或者标记。
- **垃圾邮件过滤器 –** 启发式的检查电子邮件消息，这种新垃圾邮件过滤技术目的在于计算一个“分数”。这个分数用来决定一个邮件作为一个垃圾邮件的可能性。基于这种决策，服务器可以在之后采取某些行动，例如拒绝或者标记邮件。
- **SSL 和认证 –** MDaemon 支持 SMTP，POP，IMAP 和 WorldClient 的 Web 服务器的 SSL 协议。SSL 是一种安全服务器/客户端 Internet 通信的标准方案。
- **地址抑制 –** 不允许所列的地址发送邮件到您的服务器。
- **IP 屏蔽–** 用来指定您拒绝连接到您服务器的 IP 地址。
- **主机屏蔽-**用来指定您拒绝连接到您服务器的主机名称。（域名称）。
- **IP 防护 –** 如果一个在列表中的指定的域名称试图连接您的服务器，他的 IP 必须匹配您指派给他的其中之一。
- **SMTP 认证 –** 用来设置几个表示在一个用户发送消息到已经或者还没有认证的 MDaemon 时，MDaemon 将如何操作的选项。
- **在 SMTP 之前 POP –** 标签上的控制用来要求每一个用户在被允许通过 MDaemon 发送消息前，首先访问他或者她的邮箱，因此认证用户为合法帐号持有者并且允许使用邮件系统。
- **站点使用政策 –** 用来创建一个站点安全政策，以用来在没一个 SMTP 邮件

会话开始时，传递发送服务器。通常站点政策的一个范例是，“此服务器没有转发”。

- **中转设置** – 用来控制当不是来自也不是发送到的本地地址邮件到达您的邮件服务器时，MDaemon 将会做什么。
- **被信任的主机** – 域名称和 IP 地址将会被认为是在转发标签上的转发规则的例外。
- **Tarpitting** – 此功能使得您一旦从邮件发送者那里收到了大量 RCPT 命令，就可以故意的减缓一个连接。这是阻止垃圾邮件发送者试图使用您的服务器发送未请求的大批邮件（垃圾邮件）。在此技术下的这种假设是如果在发送每一个邮件时，占用垃圾邮件发送者相当长的时间，则将可以阻止他们未来试图再次使用您的服务器。
- **反向查找** – MDaemon 可以问询 DNS 服务器检查在来信时所报告的域名称和地址的合法性。在此标签上的控制可以拒绝可疑的邮件或者将特殊的邮件头插入其中。反向查找数据也可以在 MDaemon 日志中报告。

DNS黑名单 (DNS-BL)

DNS黑名单(DNS-BL)能被用于防止大多数“垃圾邮件”到达您的用户。这个新的安全特性允许您指定数个ORDB和MAPS RBL类型的主机(维护已知发送垃圾邮件服务器的列表)，这将在每次有人试图发送邮件到您的服务器时进行检查。如果连接的IP地址已经被任何这些主机列为黑名单，这个邮件将被拒绝或标记。

注意

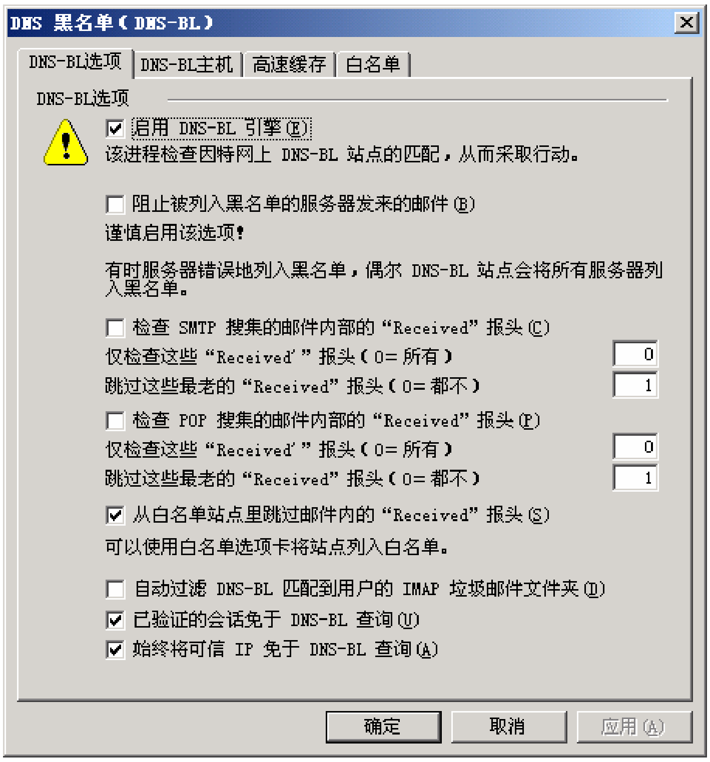
使用这个功能会阻止大部分的垃圾邮件被发送到您的服务器。然而，有些站点会被误列入黑名单，因此使用这个功能也会引起一些为难，但如果您正为控制垃圾邮件而发愁，这还是很值得的。DNS-BL查询根据在**设置>主域>DNS**中指定的DNS服务器执行。这个功能经过测试并运行良好，对每个邮件进程速度没有显著延迟。DNS黑名单包含一个“例外”数据库用于指定那些不用经过DNS-BL查找的IP地址。在激活这个功能之前，您必须将您本地的IP地址范围添加到这个免除列表中来避免查找。127.0.0.1是被免除的，因此它不必被添加到免除列表中。

更多关于垃圾邮件以及如何通过ORDB和MAPS RBL来控制和消除垃圾邮件的信息，请访问： http://www.ordb.org

http://www.mail-abuse.com/rbl/

ORDB和MAPS RBL是他们各自组织的商标。Alt-N Technologies很荣幸能与他们联合，代表我们的用户使用他们的服务。

DNS-BL选项



DNS-BL

启用DNS-BL引擎

点击这个复选框来打开DNS黑名单。

阻止从已经被列为黑名单的服务器发来的邮件

当这个选项被激活，在SMTP进程期间，MDaemon将拒绝那些经过DNS-BL查找结果证实为列入黑名单的邮件。如果您禁用/清除这个选项，从被列入黑名单的服务器收到的邮件将不会被拒绝，但是将获得一个X-RBL-警告：嵌入到邮件标题中。您可以使用内容过滤器的特性来搜索拥有此类标题的邮件，并根据您的需要来处理它们。

更多信息，参见如下选项 *“自动过滤DNS-BL匹配用户的IMAP垃圾邮件文件夹”*

在SMTP收到的邮件中检查‘接收到的’标题

点击这个开关，如果您想让DNS黑名单检查通过SMTP收到的嵌入在邮件标题中的IP地址。

检查一定数量的‘接收到的’邮件标题 (0 = 所有)

指定您想DNS-BL检查最近*‘接收到的’*邮件标题的数目。数值“0”意味着所有接收到的邮件标题将被检查。

忽略一定数量的最先'接收到的'邮件标题 (0 =没有)
使用这个选项，如果您想在检查SMTP邮件时，让DNS-BL忽略一个或多个'*接收到的*'邮件标题。通常这非常有必要用于忽略最早'*接收到的*'邮件标题，这个选项默认设置是“1”。

在POP收到的邮件中检查'接收到的'邮件标题
当这个开关被打开时，DNS-BL将在通过DomainPOP和MultiPOP收到的邮件中检查'*接收到的*'邮件标题中含有的IP地址。

检查一定数量的接受到的邮件标题(0 = 所有)
指定您想让DNS-BL检查的最近接收到的邮件标题的数目。数值“0”意味着所有接收到的邮件标题将被检查。

忽略这些数量的最早'接收到的'邮件标题(0 =没有)
使用这个选项，如果您想让DNS-BL在检查DomainPOP和MultiPOP邮件时忽略一个或多个'接收到的'邮件标题。通常很有必要忽略最早的'接收到的'邮件标题，这个选项的默认设置是“1”。

忽略被免除的IP地址处发出邮件中的'接收到的'邮件标题
当这个选项被激活，DNS-BL不会检查您指定的被免除的IP地址处发出邮件中的'接收到的'邮件标题。点击如下的“例外”按钮来指定那些IP地址。

自动过滤DNS-BL匹配用户的IMAP垃圾邮件文件夹

点击这个选项将会创建一个“`Inbox\Spam\`” IMAP文件夹用于所有将来您添加到MDaemon的用户帐号。MDaemon还会每个用户创建一个IMAP邮件规则，这将搜索`X-RBL-Warning`标题并将包含该标题的邮件放置到用户的垃圾邮件文件夹。当您点击这个选项，您将被问及是否您想让MDaemon来为每个您现存的用户帐号创建这个文件夹和规则。参见下面*为每一个账户自动生成一个垃圾邮件文件夹和规则*

为每一个账户自动生成一个垃圾邮件文件夹和规则

MDaemon能为每一个账户自动创建一个“`Inbox\Spam\`” IMAP邮件文件夹，并生成一个 IMAP邮件规则，那就是任何时候只要发现`X-RBLWarning`邮件标题就会将邮件转移到那个文件夹中。无论何时您点击上面的选项，您将看到一个选项为所有账户创建文件夹和规则。只要在对话框中选择“是”就能创建文件夹和规则。这是个简单和可靠的方式来帮助您的用户快速识别垃圾邮件—它能有效阻止垃圾邮件与其他合法邮件混淆。他们只需要偶尔察看一下他们垃圾邮件文件夹的内容来确信没有任何重要邮件被意外地放置其中 (这种情况有时候会发生)。当为您的帐号创建文件夹和规则时，如果MDaemon发现有帐号已经拥有规则来检查`X-RBL-Warning`邮件标题的存在，那么对那个账号就不会采取任何动作也不

会创建任何规则。如果您想要定义IMAP文件夹的名称不是“垃圾邮件”，您可以通过编辑下面MDaemon.ini文件中的键值来改变这个默认设置：

[Special]
DefaultSpamFolder=Spam (Replace “Spam” with another name - 20 chars maximum)

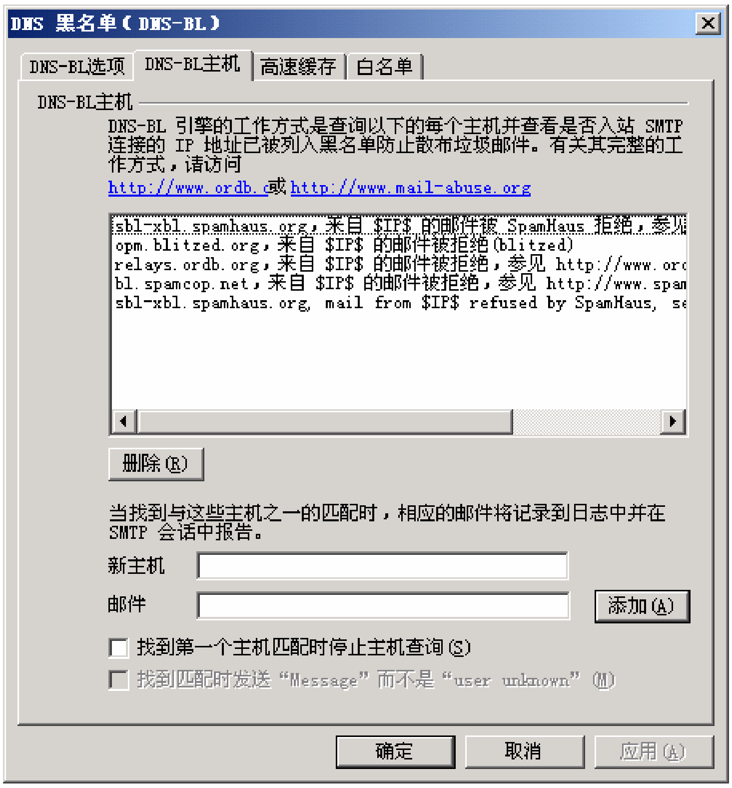
被验证的进程免于DNS-BL 查找

选中这个复选框，如果您想让那些使用AUTH命令进行验证的进程被免除DNS-BL查找。

总是免除被信任的IP地址被DNS-BL查找

点击这个复选框，如果您想让被列在传递设置的被信任的主机标签上的地址免受DNS-BL 找。

DNS-BL主机



DNS-BL

MDaemon将在对一个特定IP地址执行DNS-BL查找时查询每个主机。如果一个主机响应查询为一个正面的结果，MDaemon将拒绝从那个IP地址接收邮件，并将发送被列入黑名单的主机地址的相关信息的短消息。(如果您已经激活了如下的“发送匹配的邮件…” 选项)。

注意
如果您已经选择将邮件标记成垃圾邮件(参见DNS-BL选项标签中的选项)，MDaemon在SMTP进程期间将不会拒绝一个发送到有效用户的邮件，如果发现黑名单匹配也不会发送一个RBL主机或“未知用户”消息。

删除
从RBL主机列表中选择一个条目并点击这个按钮将其从列表中删除。

添加新的主机t
如果您想添加新用来查询黑名单IP地址的主机，请在此输入。

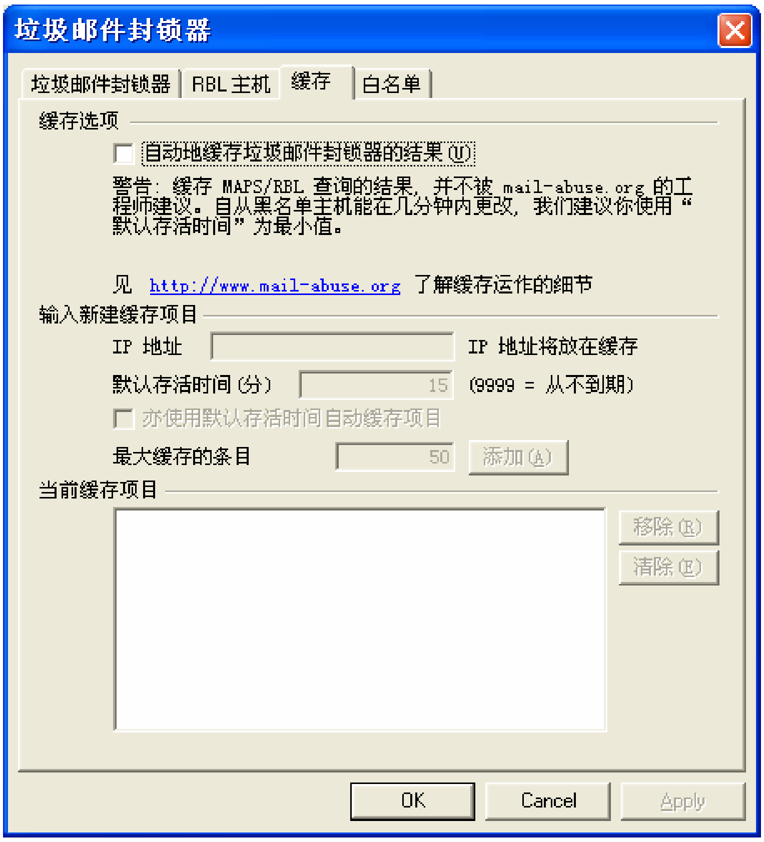
通知
这是当一个IP地址被新的主机列为黑名单时将要发送的通知消息。

添加
在输入一个新的主机和通知消息后，点击这个按钮来将其添加到RBL主机列表。

在首次主机匹配时停止主机查询
经常有很多主机被包含在DNS-BL处理的每个邮件的邮件头中，多个RBL主机被查询。通常，DNS-BL将对所有的邮件中的主机继续查询RBL主机，不论发现多少个匹配。点击这个选项，如果您想在发现任何匹配后让DNS-BL对任何给出的邮件停止RBL主机查询。

发送匹配“邮件”而不是 “未知用户”
选中这个选项，如果您想让特定RBL主机的信息在SMTP进程期间发送给对方，当其IP地址是否被列入黑名单。否则，一个“未知用户”消息将被发送。如果您已经选择使用DNS-BL选项标签上的选项来标记垃圾邮件而不是拒绝它们，这个选项将不可用。

缓存



缓存选项

自动缓存垃圾邮件封锁器的结果

如果您希望缓存那些从垃圾邮件封锁器查找中收到的一个肯定（例如黑名单）结果的 IP 地址，那么请启用此功能。

警告：
尽管缓存地址可能会保存一些资源，但是由于垃圾邮件拦截器不将需要对那些已经被缓存的 IP 地址执行查询 – 它并不被 RBL 主机所推荐。有一个黑名单 IP 地址可能将它的状态在大概几分钟内进行修正，缓存条目可能导致非必要邮件被拒绝。如果您选择使用此功能，则我们推荐保持任何被缓存的条目的时间尽量小。更多缓存垃圾邮件封锁器查找的关联信息，请参看 www.mail-abuse.org。

输入新建缓存条目

IP 地址

输入您希望手动添加到垃圾邮件封锁器缓存中的 IP 地址。

默认存活时间（分钟）

这个量是条目将保留在垃圾邮件封锁器缓存的时间量。输入 9999 到这个区域将会阻止条目过期 – 但是并不推荐这么做。

亦使用默认存活时间自动缓存项目

如果您希望使用以上指定的默认活动时间设置来自动缓存条目，点击此复选框。正常情况下，TTL 参数是基于 DNS 查找期间返回的信息，而不是默认活动时间设置。

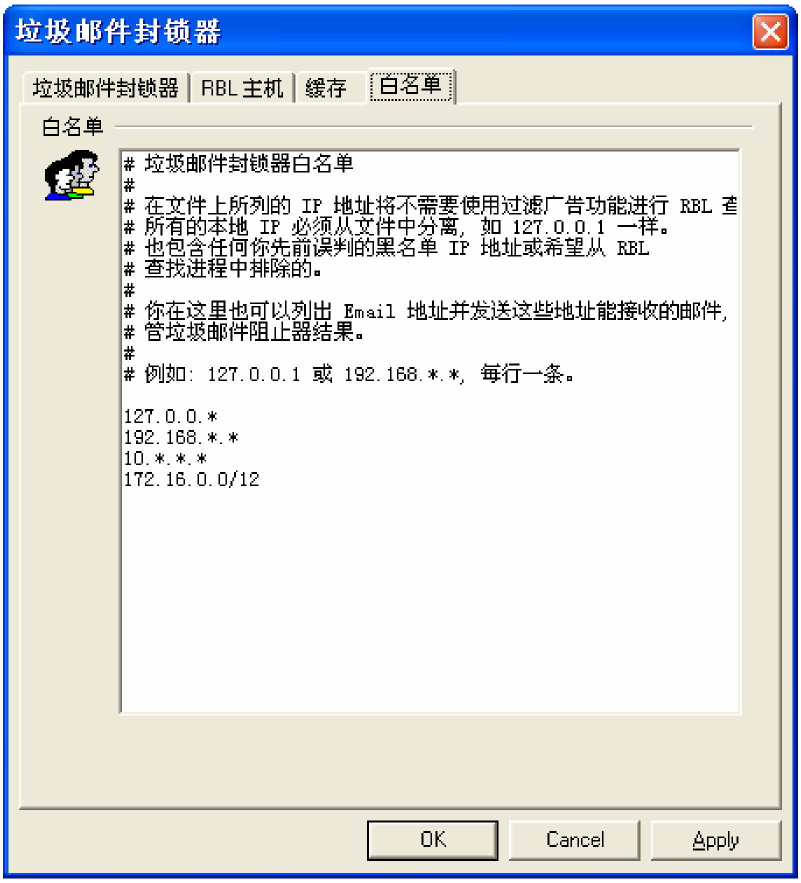
最大缓存的条目
这是您希望允许被缓存的条目的最大数量。

添加
在输入 IP 地址和默认活动时间后，点击此按钮添加条目到缓存 IP 地址列表中。

移除
选择一个条目，然后点击此按钮从混存地址列表中移除它。

清除
点击此按钮，清除所有缓存的 IP 地址列表。

白名单列表



白名单列表

使用此标签，指定从垃圾邮件封锁器查找中将被免除的 IP 地址。您应该总是包括您的本地 IP 地址范围来阻止垃圾邮件封锁器查询来自本地用户域的邮件（如 127.0.0.1，192.168.*.*及其它）。在每一行上放置一个地址。允许通配符。

垃圾邮件过滤器

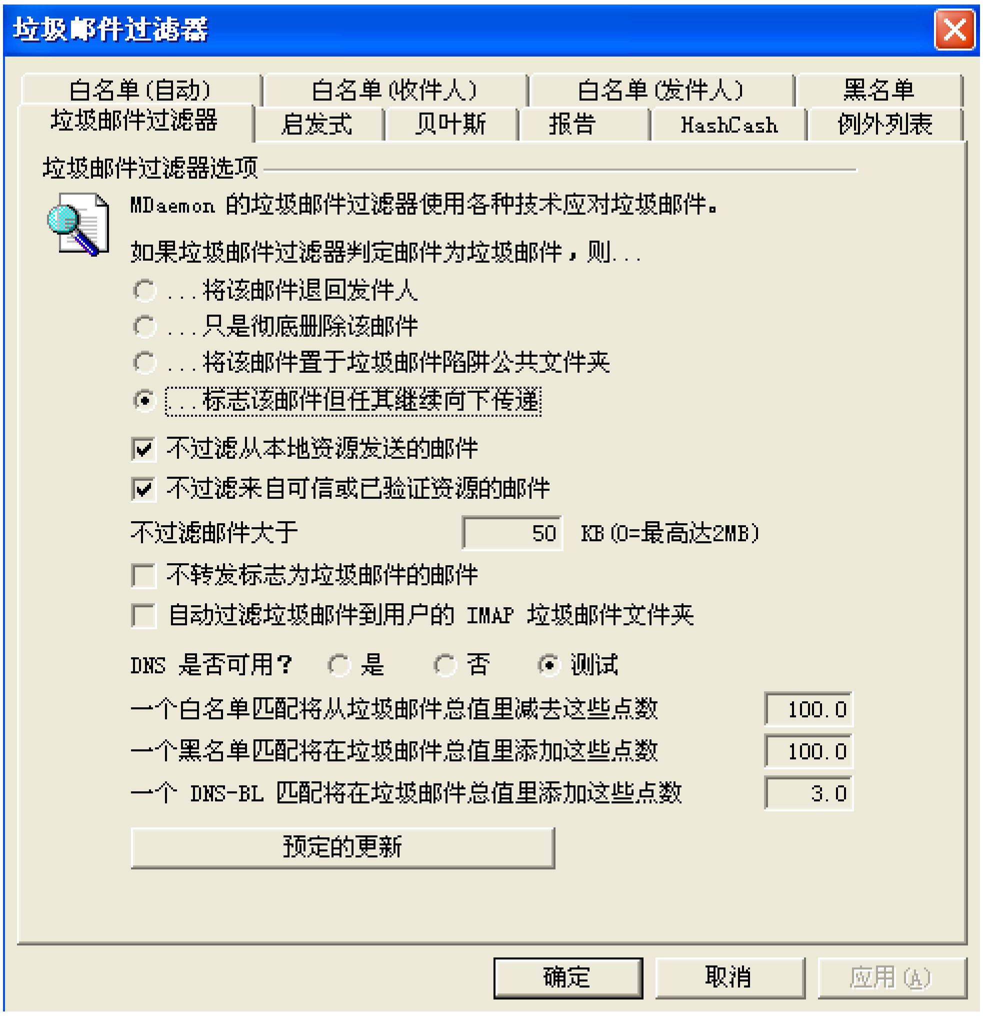
垃圾邮件过滤器增强了 MDaemon 已扩展的垃圾邮件阻止工具套件。垃圾邮件过滤器应用新技术用来严格检查来信，目的是为了计算基于“分数”的系统规则。这个分数之后用来检查一封邮件作为垃圾邮件的可能性，以及可以基于此分数而实施的某些操作 – 您可以拒绝消息或者将其作为可能的垃圾邮件标记。

地址可以列入白名单或黑名单中，或者指定成在垃圾邮件过滤器检查中完全免除。您可以生成一个垃圾邮件报告插入到邮件中，显示它们的得分和那些分数如何得到，或者您可以生成一个单独的电子邮件而使原来的垃圾邮件将其作为附件包含。而且，您甚至可以使用贝叶斯学习来帮助垃圾邮件过滤器随时间学习更准确的区分垃圾邮件并由此增加它的可靠性。

最后，通过检查许多成千的已知垃圾邮件和检查垃圾邮件特征，规则随时间优化而且非常可靠。但是，您可以通过编辑垃圾邮件过滤器配置文件自定义或者添加新规则来满足特别的需要。MDaemon 垃圾邮件过滤器使用整合的，流行的开放源代码的科技。

开放源代码项目主页在 http://www.spamassassin.org。

垃圾邮件过滤器



垃圾邮件过滤器选项

如果垃圾邮件过滤器判断一个邮件是垃圾邮件，则...

如果一个邮件的垃圾邮件分数比在启发式中设定的垃圾邮件分数高或者相同的话，垃圾邮件过滤器将会采取以下操作。

...把此已经返回给发送者

如果您希望试图弹回每一个垃圾邮件邮件到它的发送者，选择此选项。垃圾邮件由于具有不合理回复路径，所以这些消息可能经常无法投递。

...完全删除邮件

如果您希望简单的删除所有那些垃圾邮件分数超过指定极限的来信，请选择此选项。

...标记邮件，但让它继续沿路径发送

如果您希望让其继续发送每一个垃圾邮件到其指定的收件人，并且通过插入在启发式标签上设定的垃圾邮件邮件头和/或标签来标记其为垃圾邮件，那么请选择此选项。

…把邮件放到垃圾邮件公共文件夹中

如果您希望将邮件标记为垃圾邮件，然后移动它们到垃圾邮件公共文件夹而不是允许它们发送，那么请选择此选项。

不过滤从本地源发送的邮件

如果您希望从本地用户和域中发送的消息不被垃圾邮件过滤器过滤，请选择此选项。

不过滤从信任的或认证源的邮件

如果您希望从信任的域或者已认证的发送者发送的消息不被垃圾邮件过滤器过滤，请启用此选项。

不过滤邮件大于 xxkb（0=up to 2 megs）

由于通常垃圾邮件发送者的目标是在最短的时间内发送尽可能多的消息，因此很典型垃圾邮件消息通常都非常小。如果您希望大于某一尺寸的邮件被垃圾邮件过滤器免除，则在此指定文件大小（KB 为单位）。如果您不希望大小作为邮件过滤器决定垃圾免除的要素之一 – 不论大小消息都将被垃圾邮件过滤器所处理，请使用值“0”。

不发送标记为垃圾邮件的邮件

如果您不希望允许垃圾邮件被转发，点击此复选框。

把垃圾邮件自动过滤到用户的 IMAP 垃圾邮件文件夹

点击此选项，MDaemon 将会自动放置每一个垃圾邮件过滤器决定为垃圾邮件的邮件到每一个用户的“垃圾邮件”IMAP 文件夹中（如果此文件夹存在）。它将会为每一个添加的新用户帐号自动创建文件夹。

当您点击此选项，您将被询问您是否想要 MDaemon 为每一个您已经存在的用户的帐号创建此文件夹。如果您选择“是”，则将会为所有用户创建一个文件夹。如果您选择“否”，则只有在添加每一个新用户时，才会创建文件夹。任何已经存在的，为部分或者所有用户的文件夹都不会被改动或者受到任何影响。

匹配白名单，则从垃圾邮件分数减去

在垃圾邮件过滤器白名单上包含的一个地址不能保证来自或发送到该地址的邮件不被自动当成垃圾邮件。取而代之的是，白名单所列的地址将会使在他们的垃圾邮件分数上减去此此指定的分数。例如说，如果您的垃圾邮件分数极限设置成 5.0，而此数值设置成 100，如果一封垃圾邮件邮件在白名单分数值被减前，到达邮箱得到 105.0 的垃圾邮件分数或者更高，则该消息的最终垃圾邮件分数将会至少为 5.0 – 因此将其作为垃圾邮件隔离。但是由于垃圾邮件几乎不会有如此好的分数，除非它包括了其它一些额外的高分数元素，比如黑名单地址，所以这种情况几乎不会发生。当然，如果您设置白名单减值为一个很低的量，则这种情况将会经常发生。

匹配黑名单，则从垃圾邮件分数加上

就像上面的白名单选项，包括在垃圾邮件过滤器的黑名单上的地址不能保证来自该地址的消息将会被当成垃圾邮件。取而代之的是，在此控制上指定的值将会被添加到垃圾邮件的分数中，这将在之后被用来决定是否邮件是垃圾邮件。

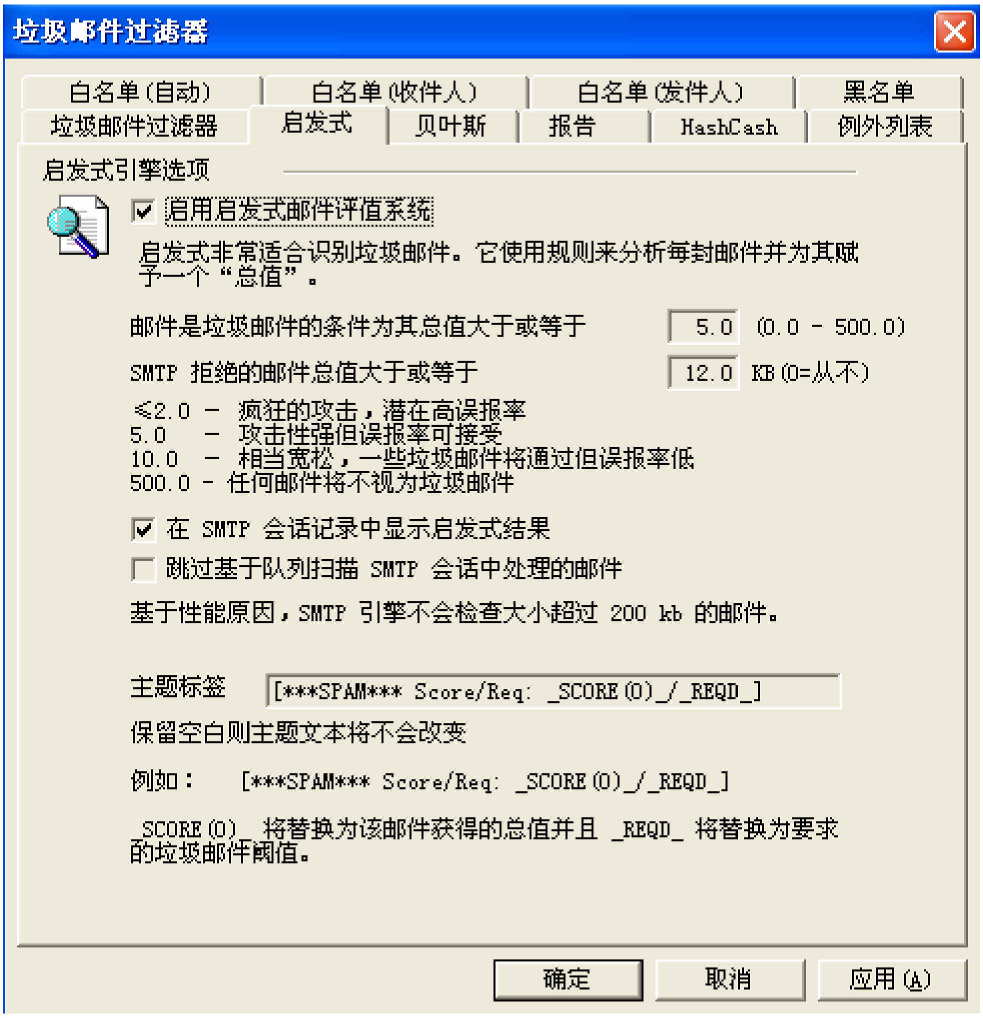
DNS 黑名单匹配，则从垃圾邮件分数加上

如果您使用 DNS 黑名单（123 页），则当 DNS 黑名单符合结果时，您可能使用此项来指定一个将被添加到邮件的垃圾邮件分数中的值。有时，垃圾邮件过滤器的邮件的启发式检查不会使其分数高到足以被认为是垃圾邮件，但是一个 DNS 黑名单检查可能会显示其可能使垃圾邮件。加上此值到这些邮件的垃圾邮件分数中可以帮助减少垃圾邮件的数量，并设法处理那些漏过垃圾邮件过滤器发现的邮件。

日程表更新

点击此按钮来打开 AntiSpam 更新事件安排对话框（设置 – 事件安排…），您可以在其上安排垃圾邮件过滤器检查启发式引擎文件更新的时间。

启发式



启发式引擎选项

启用启发式邮件评分系统

点击此复选框启用启发式邮件分数，垃圾邮件过滤器系统。在此选项启用前，没有任何标签上的垃圾邮件过滤器选项可以使用。

邮件是垃圾邮件，如果分数超过或等于 ***xx*** *（****0.0 - 500.0****）*

您在此指定的这个值是垃圾邮件的阀值，会被 MDaemon 用来比较每一个邮件的垃圾邮件分数。任何具有高于或者等于此值的分数的邮件将会被当作垃圾邮件，然后将会实施在垃圾邮件过滤器设置适用的操作。

SMTP *邮件被拒，分数超过或等于* ***xx*** *（****0=****永不）*

使用此选项指定垃圾邮件分数拒绝阀值。当一个邮件的垃圾邮件分数高于或者等于此值时，它将会被完全拒收，而不是仅仅通过被剩余部分处理并投递。此选项的此值应该总是高于"*如果一个消息的垃圾邮件分数…*"这个选项的值。否则，一个邮件将绝不会当成垃圾邮件，并且垃圾邮件过滤器选项的其他部分将对其应用 – 它将在投递时被轻易拒绝。如果您希望不论邮件分数如何，Mdaemon 都不会拒绝任何邮件，那么请在此选项中使用"0"。

例子，

如果您将垃圾邮件分数极限设置为 5.0，而拒收极限设置为 10.0，那么任何具有高于或等于 5.0 但低于 10.0 垃圾邮件分数的消息都将被当成垃圾邮件，并且将通过垃圾邮件过滤器并有对话框上的其他设置来处理。任何具有高于或者等于 10.0 垃圾邮件分数大额消息都将在投递过程中被 MDaemon 拒绝。

注意：
您应该随时监视垃圾邮件过滤器的性能，并且精炼垃圾邮件和拒收阀值以适应您的需要。然而，对于更多人，5.0 这个垃圾邮件分数阀值能捉住更多的垃圾邮件，只具有极少漏检（垃圾邮件未被识别）并且几乎没有任何误判（邮件被错误的认为垃圾邮件）。10 或者 15 的拒绝阀值将会是只有几乎确认为垃圾邮件的消息被拒绝。

注意：
通常，当一个邮件由于其分数过高被拒绝时，邮件的细节不会被记录下来。然而，您可以改变在 CFILTER.INI 文件中的以下键值，就可以使这些细节被记录到 SMTP 日志中（不是垃圾邮件日志）： [SpamFilter] InlineSMTP=Yes

在 ***SMTP*** *会话记录显示启发式结果*

点击此选项显示在 SMTP 会话中显示的启发式处理结果。此选项在您将您的垃圾邮件分数拒绝极限设置为"0" 时 – 意味着垃圾邮件将不会由于它的分数被拒绝，是不可用的。更多信息，参看上文中的 *SMTP 邮件被拒，分数超过或等于 xx（0=永不）*。

当检测到垃圾邮件时在 "主题" 中插入标签

如果您希望任何达到或者超过垃圾邮件分数的邮件都有一个指定标签插入到它的主题邮件头中，请点击此复选框。这个标签将包含垃圾邮件分数的信息，您可

以使用您的 IMAP 消息过滤器来查询它，从而过滤它。对自动路由垃圾邮件邮件到指定的“垃圾邮件”文件夹来说，这是一个简便的方法。

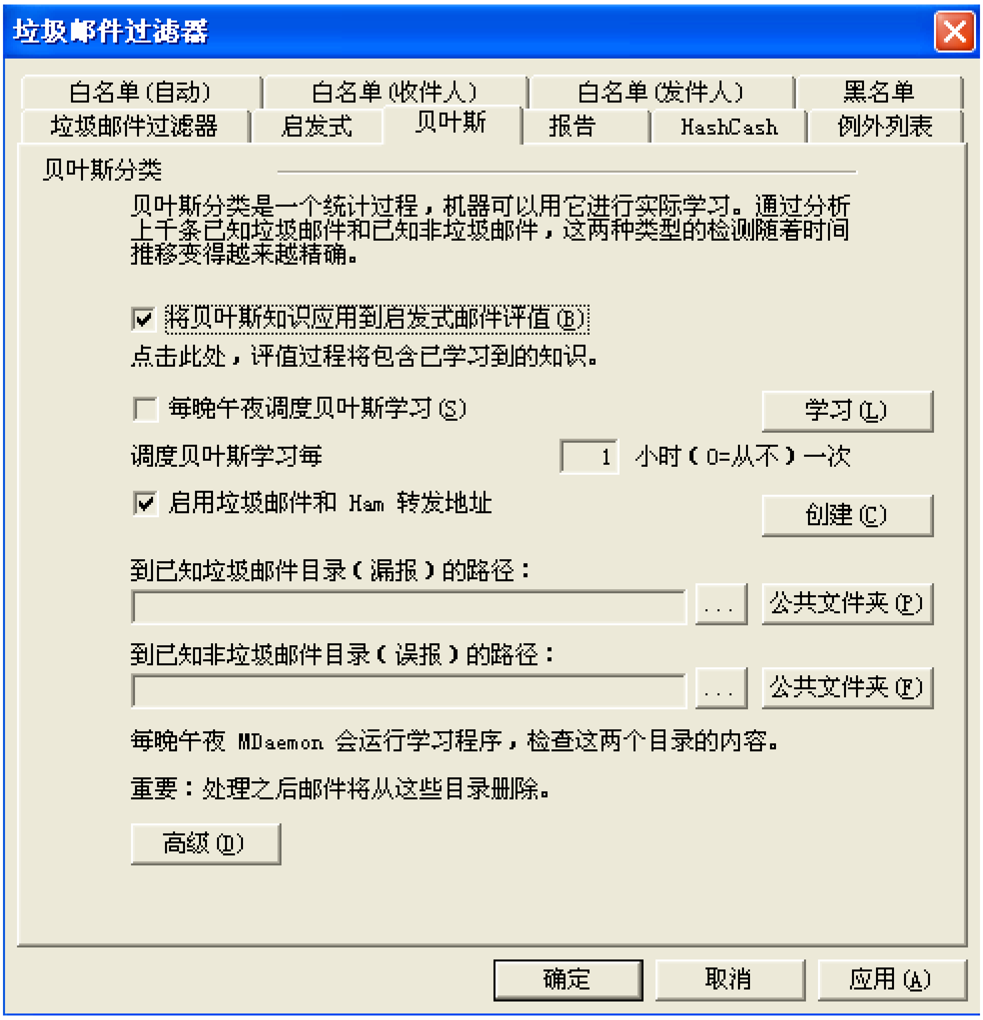
主题标签

这个标签将会插入到所有达到或者超过所要求的垃圾邮件分数极限的邮件的主题邮件头的开始部分。如果您希望动态插入消息的垃圾邮件分数和所需的垃圾邮件极限的数值，则为消息的分数使用标签“_HIT_”，为所需的极限使用“_REQD_”标签。

例子，

主题标签设置为：***SPAM*** Score/Req：_HITS_/_REQD_ - 将会使得垃圾邮件消息得到 6.2 分数，主题为“嘿，这是些垃圾邮件！”改为“***SPAM*** Score/Req：6.0/5.2 - 嘿，这是些垃圾邮件！”。

贝叶斯



垃圾邮件过滤器支持贝叶斯（贝叶斯）学习，这是一个统计学处理过程，可选的用于分析垃圾邮件和非垃圾邮件，以增加垃圾邮件识别的可靠性。您可以每天午夜扫描垃圾邮件和非垃圾邮件指定的文件夹。在那些文件夹中的所有邮件将会被

分析并索引以致和新邮件能够统计性的进行比较，以便于决定他们是垃圾邮件的可能性。垃圾邮件过滤器可以基于贝叶斯比较结果增加或者减少一个邮件的垃圾邮件分数。

注意：
垃圾邮件过滤器将不会应用贝叶斯分类到邮件，直到贝叶斯已经分析了在贝叶斯高级对话框上指定的一定数量垃圾邮件和非垃圾邮件（点击此标签上的高级进入对话框）。这对于在做贝叶斯比较时，垃圾邮件过滤器有足够的统计来作出可靠的结果，是非常必要的。一旦您送给系统一封邮件去分析，它将有足够的准备开始将贝叶斯比较的结果应用到每一个来信的垃圾邮件分数中去。通过继续分析更多的邮件，贝叶斯分级将随着时间变得更为精确。

贝叶斯分类

把贝叶斯知识应用到启发式邮件分数中

如果您希望每一封邮件的垃圾邮件分数在贝叶斯统计比较的基础上进行调整，点击此选项。

启用贝叶斯计划学习

如果您希望垃圾邮件过滤器分析所有包含在以下指定文件夹中的邮件，激活此选项。这些文件夹的内容将会每一天的午夜分析一次，然后删除。

注意：
如果您不希望邮件在它们被分析之后删除，则您可以通过复制 LEARN.BAT 到\MDaemon\App\下级文件夹中的 MYLEARN.BAT 来阻止，之后在那个文件中删除以“del”开头的两行。当 MYLEARN.BAT 文件在那个文件夹中时，MDaemon 将会使用它替代“LEARN.BAT”。参看在您的\MDaemon\SpamAssassin\文件夹中的 SA – Learn.txt，以得到更多信息。更多启发式垃圾邮件过滤技术和贝叶斯学习的细节，请访问 http://www.spamassassin.org/doc/sa-learn.html

学习

点击此按钮，对指定的文件夹进行一个手动的贝叶斯分析，而不是等待午夜的自动分析。

启用垃圾邮件和非垃圾邮件转发地址

如果您希望允许用户转发垃圾邮件和非垃圾邮件（ham）邮件到指定地址，以便贝叶斯系统可以从它们中学习，那么点击此复选框。MDaemon 将会使用的默认地址时“SpamLearn@<domain.com>和“HamLearn@<domain.com>”。送到这些地址的邮件必须通过 SMTP 认证会话中被接收。而且，Mdaemon 希望将邮件作为“message/rfc822”类型的附件转发到以上地址。任何其他类型被发送到这些电子邮件地址的邮件将不会被处理。

您可以通过编辑在 CFILTER.INI 文件中的以下键值来改变 MDaemon 使用的地址：

[SpamFilter]
SpamLearnAddres=SpamLearn@
HamLearnAddress=HamLearn@

注意：这些键值的最后一个字母必须为“@”。

创建

点击此按钮自动创建垃圾邮件和非垃圾邮件公共 IMAP 文件夹，为了配置 MDaemon 使用它们。将会创建以下文件夹：

<贝叶斯 Learning> - IMAP 文件夹根目录
<贝叶斯 Learning\\Spam> - 此文件夹为人工挑选的垃圾邮件
<贝叶斯 Learning\\Ham> - 此文件夹为人工挑选的非垃圾邮件

通过默认值，这些文件夹的访问权限只授于本地域的本地用户，并对查找和插入进行限制。邮件管理员的默认权限是查找，读，写，插入和删除。

到已知垃圾邮件目录（漏报）的路径：

这是存放已知的垃圾邮件文件夹的路径，它将会用来被贝叶斯分析所使用。只能复制您认为是垃圾邮件到此文件夹。由于错误的潜在性，您不应该自动复制邮件到此文件夹这个操作。自动执行这个过程可能有时会导致非垃圾邮件被作为垃圾邮件来分析，这些可能会降低贝叶斯统计的可靠性。

到已知非垃圾邮件目录（误报）的路径：

这是存放已知的非垃圾邮件文件夹的路径，它将会用来被贝叶斯分析所使用。只有您认为不是垃圾邮件才应该复制到此文件夹。由于错误的潜在性，您不应该自动操作复制消息到此文件夹这个操作。自动执行这个过程可能有时会导致垃圾邮件被作为非垃圾邮件来分析，这些可能会降低贝叶斯统计的可靠性。

公共文件夹

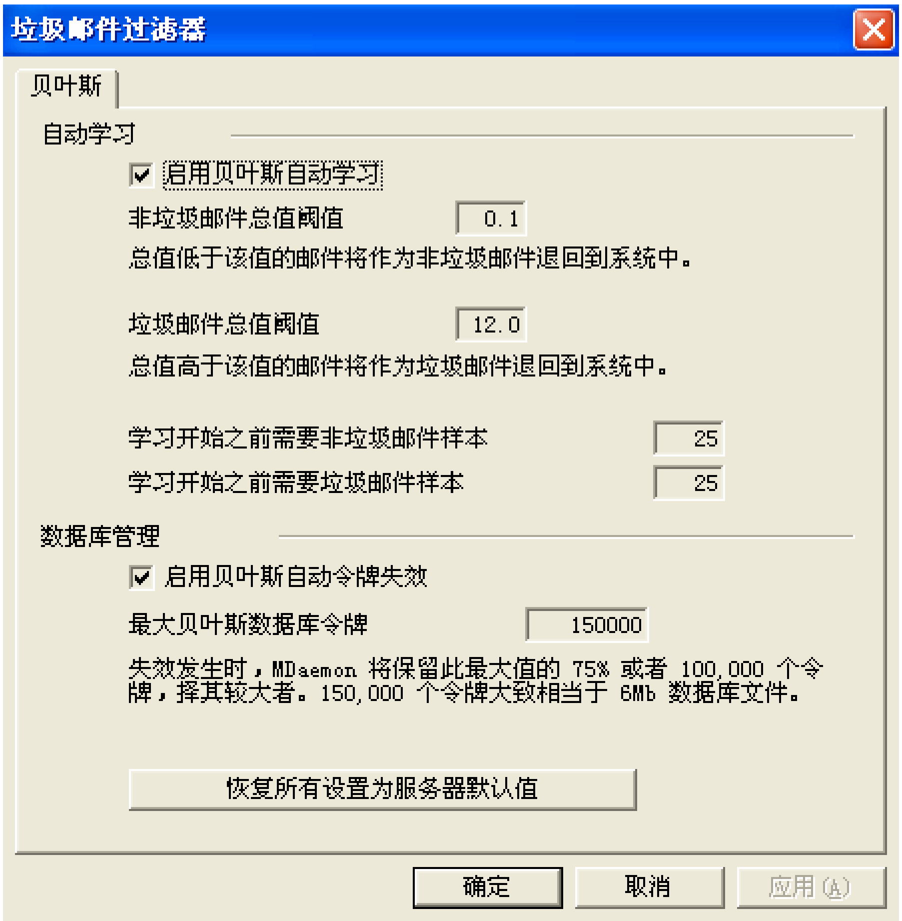
点击这些按钮之一来指定您的一个公共文件夹作为贝叶斯目录。这是为您的用户将他们的不正确分类为垃圾邮件或者非垃圾邮件消息放入到您的贝叶斯目录进行分析的简便方法。但是，请注意，让更多的人进入会增加某些邮件被放错误文件夹的可能性，因此统计的滞后性和降低可靠性。

注意：
如果您通过邮件服务器重命名一个公共文件夹，Windows Exploer 或者其他途径，则您需要手动重置这些路径到合适的新文件夹名。如果您重命名一个文件夹但没有在此改变它的路径，垃圾邮件过滤器将会为贝叶斯文件夹继续使用此路径而替代新的。

高级

点击此按钮打开贝叶斯高级选项对话框，其包含自动贝叶斯学习和指定贝叶斯数据库记号限制的选项。请看以下贝叶斯高级选项。

贝叶斯高级选项



自动学习
启用贝叶斯自动学习
利用贝叶斯自动学习，您可以指定垃圾邮件和非垃圾邮件的分值极限。任何分数在非垃圾邮件极限以下的邮件都将被自动学习当作非垃圾邮件对待，并且任何分数在垃圾邮件分值以上的分值都将被当成垃圾邮件对待。尽管自动学习并不被广泛推荐，但如果您小心设置极限分数，它将让您受益匪浅，这是因为它允许从数据库文件中移除得老的过期标记可以自动被替换。这样可以阻止手动训练覆盖过期标记的需求。

非垃圾邮件计分临界值
具有此数值以下的垃圾邮件分数的邮件将会被贝叶斯分级系统当作非垃圾邮件。

垃圾邮件计分临界值
具有此数值以上的垃圾邮件分数的邮件将会被贝叶斯分级系统当作垃圾邮件。

在学习启动前需要非垃圾邮件采样
垃圾邮件过滤器不会应用贝叶斯分级到邮件中，直到此数量的非垃圾邮件（和下一个选项中指定的垃圾邮件）已经被贝叶斯系统所分析。为了让垃圾邮件有一个足够的统计池来作贝叶斯比较，这是非常必要的。一旦您提供系统这些邮件来分析，它将被配置得非常有效来应用贝叶斯比较的结果到每一个来信的垃圾邮件分

数中。通过连续的分析更多的消息，贝叶斯分析将会随着时间变得更为精确。

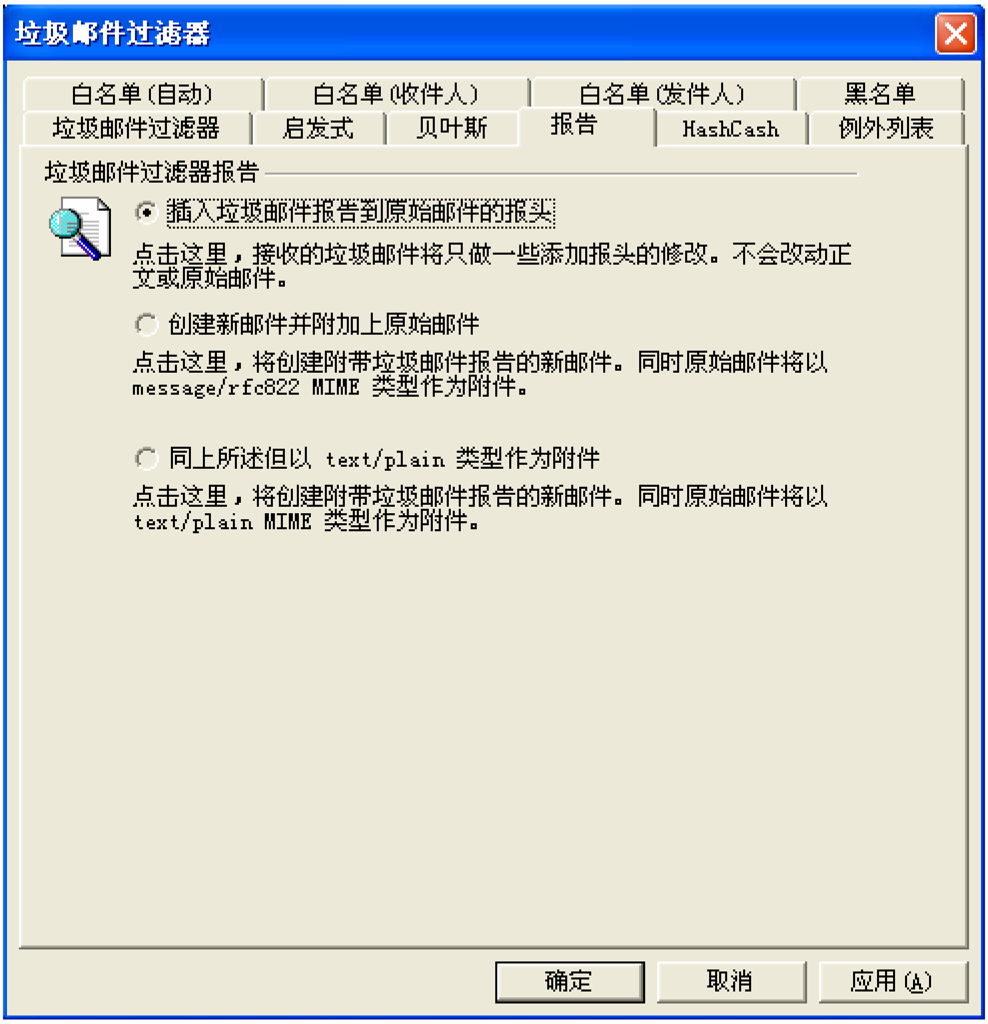
垃圾邮件采样请求，在学习启动前
就象上一个选项应用到非垃圾邮件，此选项是为了必须在垃圾邮件过滤器开始应用贝叶斯分级到垃圾邮件之前，指定垃圾邮件的数量。

数据库管理
启用贝叶斯自动标记过期
如果您希望无论何时以下指定的标记数量达到与否，贝叶斯系统都能自动过期数据库标记，那么请点击此选项。设置一个标记极限可以阻止您的贝叶斯数据库过度变大。

最大贝叶斯数据库标记
这是允许的贝叶斯数据库标记的最大数量。当达到此数量的标记时，贝叶斯系统移除最旧的，降低到此数值的 75%，或者 100，000 个标记，取二者最高的。不论有多少标记过期，标记的数量都决不会低于那两个数值中最大的。注意：150，000 数据库标记约为 8MB。

把所有设置恢复为服务默认
点击此选项恢复所有贝叶斯高级选项到它们的默认值。

报告



垃圾邮件过滤器报告

插入垃圾邮件报告到原始邮件的报头

如果您希望垃圾邮件过滤器插入一个垃圾邮件报告到每一个垃圾邮件的邮件头中，选择此报告选项。以下是一个简单的垃圾邮件报的例子：

X-Spam-Report: ---- Start Spam Filter results

5.30 points, 5 required;

* -5.7 -- Message-Id indicates the message was sent from MS Exchange

* 2.0 -- Subject contains lots of white space

* -3.3 -- Has a In-Reply-To header

* 3.0 -- Message has been marked by MDaemon's Spam Blocker

* 2.9 -- BODY: Impotence cure

* 2.2 -- BODY: Talks about exercise with an exclamation!

* 0.5 -- BODY: Message is 80% to 90% HTML

* 0.1 -- BODY: HTML included in message

* 1.6 -- BODY: HTML message is a saved web page

* 2.0 -- Date: is 96 hours or more before Received: date

---- End of Spam Filter results

创建新邮件，并附加上原始邮件

如果您希望垃圾邮件可以使创建新的电子邮件时包含此垃圾邮件报告，请选择此报告选项。原始垃圾邮件将会作为一个文件附件包含在其中。

同上所述但以 text/plain *类型作为附件*

就像前面的报告选项，这个选项将生成垃圾邮件报告成为一个包括原始垃圾邮件作为附件的新消息。不同点是原始邮件在附属时使用 text/plain MIME 类型。这是因为垃圾邮件有时包括 HTML 代码，这对每一个邮件来说是唯一的，并且可以潜在的显示哪些垃圾邮件发送者的电子邮件和 IP 地址，这种方法通过转换 HTML 代码到 plain text，就可以可以阻止那些情况的发生。

HashCash

HashCash是一项“proof of work”系统，它既是一个反垃圾邮件工具也是一个类似于电子邮票的拒绝服务对策。使用了HashCash系统，MDaemon能制造HashCash邮票，他的作用并不在于实际的游资，而是耗费一定的CPU处理时间。一个HashCash邮票被插入到一个被发出的邮件标题中，然后被收件人的邮件服务器验证并根据邮票值分别权衡。被加上邮票的邮件更可能被认为是合法的并通过收件人的服务器的反垃圾邮件系统。使用HashCash邮票能帮助减少错误并防止邮件由于未能通过一个内容过滤器或黑名单系统而被错误地拒绝。

垃圾邮件发送者依靠在极短的时间内发送成千上万的邮件的能力，以及通常使用BCC和类似技术发送一个单独的邮件给众多收件人，对任何收件人来说这不需要大量的处理时间。垃圾邮件发送者企图使用HashCash系统，然而，这需要每次为每个收件人都制造一个独特的HashCash邮票。对典型的垃圾邮件发送者而言，这将使他们的行为变得极度不可行和低效。相反，对于典型的合法邮件服务器和发件人来说，因为发送邮件而产生的额外的CPU消耗时间从根本上来说是可以忽略的，也不会以任何察觉得到的方式影响邮件的发送速度或邮件的处理时间，特别是外发邮件从不被加上邮票。邮票仅仅生成在制造列表上指定的地址中发出或收到邮件上，并且它们绝不会生成在邮件列表邮件上。再者，MDaemon的默认设置将仅当邮件通过一个经过验证的SMTP进程时生成这些HashCash邮票。需要经过验证的进程是推荐的，但也是可选项。您可以禁用，如果您想给到达未经验证的进程的邮件加上邮票。对于收到的邮件，仅有那些被指定在有效列表上的收件人收到的邮件中的邮票将被检查是否有效。如果一个接收到的邮件包含了一个HashCash邮票，但是收件人不在列表上，那么邮票将被忽略，邮件将被正常处理就如同根本没有被加上邮票一样。默认情况下，仅有您的主域包含在列表中。点击*确认列表按钮，如果您想为其添加二级域或域网关。*

更多关于HashCash的信息，请访问http://www.hashcash.org/。

HashCash

*制造和插入**HashCash**邮票到发出的邮件中*
点击这个复选框来激活HashCash系统。MDaemon将为在制造列表中指定的地址处发出或收到的外发远程邮件生成邮票。

***…**仅当邮件通过验证的**SMTP**进程*
点击这个复选框，如果您想仅为那些通过经过验证的SMTP进程到达的邮件生成邮票。清除这个复选框，如果您不需要通过验证，但不推荐这个做法。

制造列表
点击这个按钮打开制造列表。MDaemon将仅为在这个列表上的地址生成HashCash邮票。默认设置下，仅有您的主域被列其中。如果您想为您的二级域，域网关或特定个人处收发的邮件生成邮票，您需要添加这些地址到列表中。

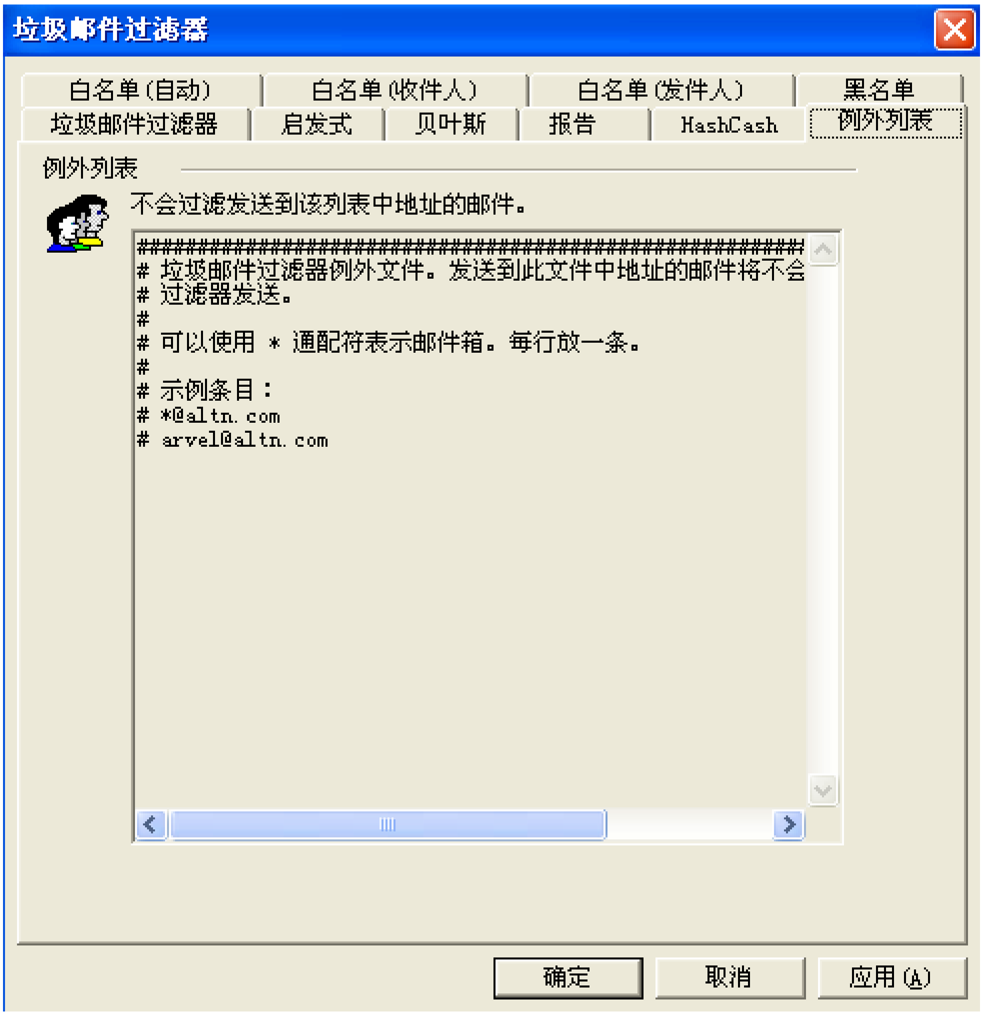
*制造如下位数的邮票**(10-32)***
这是MDaemon生成HashCash邮票时将使用的位数。位数越大，生成邮票所需的处理时间越长。

测试
点击这个按钮来测试生成指定位数的邮票所需的时间。

*检查入站邮件的**HashCash**邮票*
激活这个选项，如果您想检查入站邮件的HashCash邮票并根据结果调整它们的垃圾邮件分值。仅有那些在确认列表上指定的收件人的邮件将被检查。如果一个入站邮件包含HashCash邮票，但收件人不在列表上，那么邮票将被忽略，邮件将被正常处理就好像根本没有包含HashCash邮票一样。

确认列表
MDaemon仅将尝试确认在确认列表中指定的收件人邮件的邮票。收到的邮件如果收件人不在列表中，将被正常处理。不会执行任何HashCash邮票检查。默认情况下，只有您的主域被列入其中。

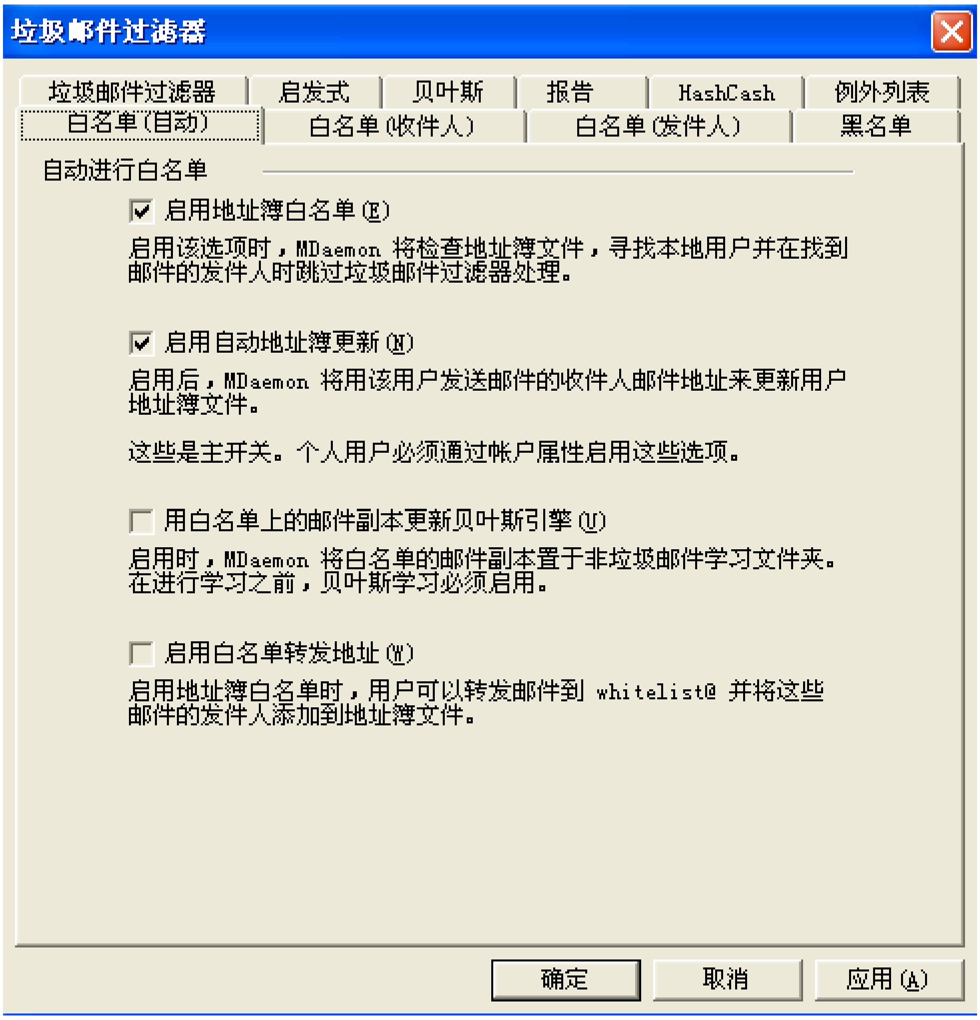
例外列表



发送到此列表中地址的邮件不会被过滤

使用此标签可以指定您希望从垃圾邮件过滤中免除的收件人地址。发送到这些地址的消息将不会被垃圾邮件过滤器处理。

白名单（自动）



自动白名单

启用地址薄白名单

点击此选项自动添加私人地址薄条目到白名单。使用此选项，MDaemon 可以通过每一个来信查询每一个用户的私人地址薄文件。如果消息的发送者在收件人的地址薄文件中，则消息将会自动被列入白名单。如果您不希望自动应用白名单列表到每一个用户，之后您可以通过清空账户编辑器中选项标签中*使用个人地址薄作为垃圾邮件过滤器白名单*选项来为个人用户关闭它。

保持您个人地址薄与 WorldClient，Outlook，Outlook Express，Windows Address Book 以及其他使用 Windows 地址薄的 MAPI 邮件客户端更新与同步，这可以通过使用 ComAgent 轻松设置。

启用自动地址薄更新

此选项自动添加任何您发送邮件的非本地电子邮件地址到您的地址薄 – 非本地收件人被添加到您的 XML 地址薄文件。当和*启用地址薄白名单*一起使用时，垃圾邮件的误判率会大大的降低。如果您不想*启用自动地址薄更新*到每个用户，您可以在用户帐号编辑器上设置。

注意：此选项对与使用自动回复的帐号是禁用的。

<u>用白名单列表的邮件更新贝叶斯引擎</u>

点击此选项使符合条件的邮件自动拷贝到贝叶斯非垃圾邮件学习文件夹中(在贝叶斯标签上指定)。这将为贝叶斯引擎自动提供非垃圾邮件的样本。有规律的为贝叶斯引擎提供非垃圾邮件的新的样本来分析将随这时间来提高可靠性来帮助降低误判率（如正常邮件被错误的认为是垃圾邮件)。

要满足这个功能，一封进来的邮件必须是发给一个本地用户，并且发件人在某的用户的 WorldClient 地址簿里。如果邮件外发，那收件人必须是在地址簿里。如果您不想外发的邮件来符合这个功能，可以使用记事本来编辑 mdaemon.ini 文件的如下设置：

```
[SpamFilter]
UpdateHamFolderOutbound=No (default = Yes)
```

如果一封邮件符合，他将会被拷贝到贝叶斯的非垃圾邮件学习文件夹，即使贝叶斯计划学习是关闭的。因而，当计划学习稍后开启或手动来激活，非垃圾邮件就会被学习。当然不是每封邮件符合并自动拷贝到学习文件夹里面去。当这个动能启用时，Mdaemon 会拷贝符合的邮件知道指定的数量已经达到。随后会在一定的时间间隔内拷贝单独的邮件。默认的话，最初的 25 封符合的邮件会被拷贝而后接下来每次 10 封。初始化拷贝的数量等于在*在学习启动前需要非垃圾邮件采样*的数量。如果您希望改变后来拷贝邮件的时间间隔，你可以编辑 mdaemon.ini 文件的如下设置：

```
[SpamFilter]
HamSkipCount=10 (default = 10)
```

最后，一旦一个指定数量的邮件已经拷贝，那么整个过程会重新开始—先拷贝 25 封邮件然后又是 10 封。默认，当 500 封邮件被拷贝完以后整个过程将重新开始。你可以编辑 mdaemon.ini 文件的如下设置：

```
[SpamFilter]
HamMaxCount=500 (default = 500)
```

<u>开启白名单转发地址</u>

如果你的帐号被设置*使用私有地址簿作为垃圾邮件白名单*，<u>开启此选项允许你转发邮件到 whitelist@<domain.com</u>>，Mdaemon 会把原始邮件的发件人加入到你的私有地址簿。白名单地址簿会从转发邮件的邮件头中提取。

转发到 whitelist@<domain.com>的邮件必须作为 message/rfc822 类型的附件转发，并且它们必须被 MDaemon 通过 SMTP 认证的会话中接受。转发的邮件达不到这些要求将不会被处理。

你可以通过在 CFILTER.INI 文件中的以下设置来更改 MDaemon 使用的地址：

```
[SpamFilter]
WhiteListAddress=WhiteList@
```

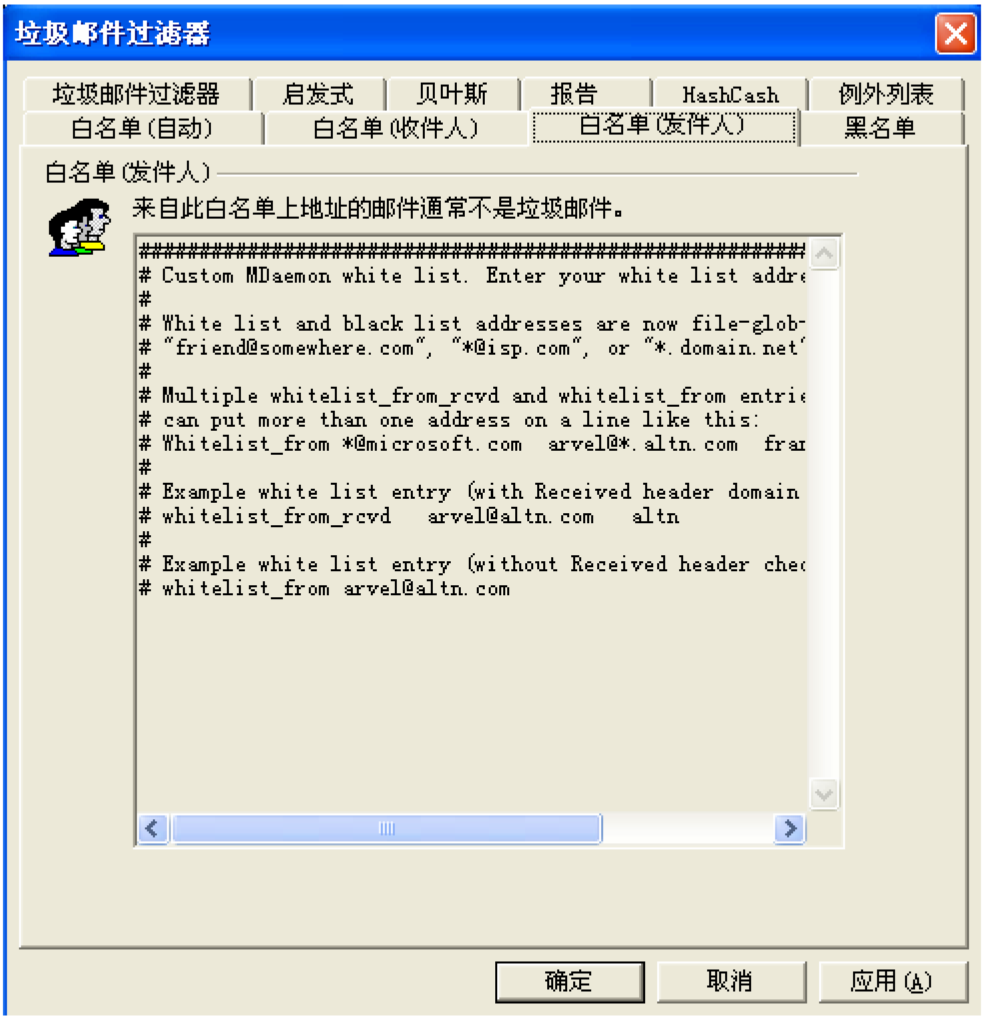
注意，最后一个字母必须为@。

白名单（收件人）

发送到此白名单上地址的邮件通常不是垃圾邮件

在此白名单上包括的地址不会保证不被当成垃圾邮件。取而代之的是，发送到白名单列表的邮件将会把垃圾邮件分数减去在垃圾邮件过滤器标签上指定的分数。例如来说，如果你将垃圾邮件极限设置为 5.0 并且在垃圾邮件过滤器上的白名单值为 50，则明显过分的垃圾邮件消息在减去白名单值前，达到 55.0 或者更高的垃圾邮件分数，之后消息的最终垃圾邮件分数将会至少为 5.0 – 因此将其分隔为垃圾邮件。但是，由于垃圾邮件几乎不会有这么高的分数，除非其包含一些例外的高分数元素，比如黑名单地址，因此这几乎不可能发生。

白名单（发件人）



来自于此白名单上地址的邮件通常不是垃圾邮件

在此白名单上包括的地址不会保证不被当成垃圾邮件。取而代之的是，从白名单列表发送的消息将会把垃圾邮件分数减去在垃圾邮件过滤器标签上指定的分数。例如来说，如果你将垃圾邮件极限设置为 5.0 并且在垃圾邮件过滤器上的白名单值为 50，则明显过分的垃圾邮件消息在减去白名单值前，达到 55.0 或者更高的垃圾邮件分数，之后消息的最终垃圾邮件分数将会至少为 5.0 – 因此将其分隔为垃圾邮件。但是，由于垃圾邮件几乎不会有这么高的分数，除非其包含一些例外的高分数元素，比如黑名单地址，因此这几乎不可能发生。

黑名单

来自于此黑名单上地址的邮件通常是垃圾邮件

在此黑名单上包括的地址不会保证当成垃圾邮件。取而代之的是，从黑名单列表发送的消息将会把在垃圾邮件过滤器标签上指定的分数加上垃圾邮件分数。例如来说，如果你将垃圾邮件极限设置为 5.0 并且在垃圾邮件过滤器上的黑名单值为 50，则明显低分值的垃圾邮件消息在加上黑名单值前，达到-50.0 或者更低的垃圾邮件分数，之后消息的最终垃圾邮件分数将不会超过 5.0 – 因此将其分隔为合法的非垃圾邮件。但是，由于消息几乎不会被从他们的垃圾邮件中减去那么多分数，除非其包含一些其他的特殊元素，比如白名单地址，因此这几乎不可能发生。

SSL和证书

MDaemon 现在对 SMTP，POP 和 IMAP，并对 WorldClient web 服务器支持 SSL/TLS 协议。有 Netscape 通信公司开发的 SSL 协议是安全服务器/客户端 Internet 通信的安全方案。它提供对 TCP/IP 连接的服务器证书，数据同步，以及可选的客户端证书。而且，由于 SSL 被内建到所有当前的主流浏览器中，简单的在你的服务器上安装一个合法的数字证书，在连接到 WorldClient 时将会激活连接着的浏览器的 SSL 能力。

如果你正在通过邮件客户端而取代WorldClient，MDaemon对SMTO和IMAP 支持在 TLS 上的 STARTTLS 扩展，以及对 POP3 支持 STLS。但是，你必须首先将你的客户端配制成为使用 SSL，以及它必须支持那些扩展 – 不是所有的邮件客户端都支持它们。

最后，你也可以为 SSL 连接限定专门的端口。这不是必须的，但可以为不支持某些 SSL 扩展的客户端提供一个更高级的可靠性。例如来说，Microsoft Outlook Express 在默认的邮件端口上不对 IMAP 支持 STARTTLS，但是它支持限定的 SSL 端口连接。

启用和配制SSL的选项在SSL&证书对话框上（点击Ctrl+L或者在MDaemon 菜单栏上的安全 – SSL/TLS/证书…）。SSL 端口设置位于主域配制对话框的端口标签上（点击 F2 或者设置 – 主域… – 端口 ）

创建和使用 SSL 证书的更多信息，请参看：

创建和使用 SSL 证书 – 161 页

更多 SSL 协议与证书的概要信息，请参看：

http://wp.netscape.com/security/techbriefs/ssl.htm

http://www.microsoft.com/technet/prodtechnol/iis/maintain/featusability/default.asp

（此连接请参看：“第六章 – 管理 Mircrosoft 证书服务和 SSL）

——

在 RFC – 2246 中有 TLS/SSL 协议，可以在此看到：

http://www.rfc-editor.org/rfc/rfc2246.txt

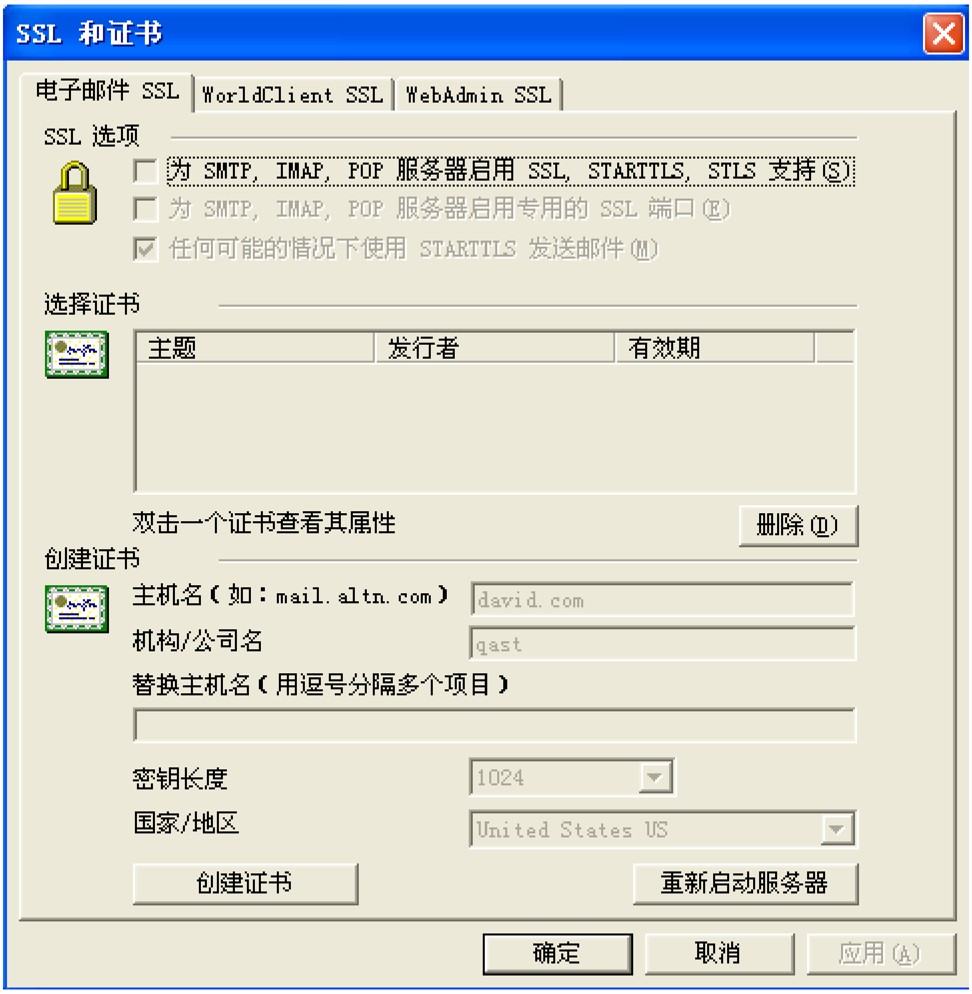
在 RFC – 3207 中有支持 SMTP 的 STARTTLS 扩展，可以在此看到：

http://www.rfc-editor.org/rfc/rfc3207.txt

在 RFC-2529 中，有利用 IMAP 和 POP 协议使用 TLS，可以在此看到：

http://www.rfc-editor.org/rfc/rfc2595.txt

电子邮件 SSL



SSL 选项

启用 SSL，STARTTLS、STLS 支持用于 SMTP，IMAP，POP 服务

点击此复选框激活对 SSL/TLS 协议，STARTTLS 以及 STLS 扩展的支持。之后，选择从以下选择证书部分中，你希望使用的证书。

启用 SMTP，IMAP，POP 服务的专用 SSL 端口

如果你希望在主域配置对话框的端口标签上的指定的专门 SSL 端口可用，点击此选项。这将不会影响客户端在默认邮件端口上使用 STARTTLS 和 STLS – 它只不过提供一个对 SSL 的附加级别支持。

任何可能的时候，使用 "STARTTLS" 发送邮件

如果你希望 MDaemon 为每一个它发送的 SMTP 消息使用 STARTTLS 扩展，点击此选项。如果 MDaemon 正在连接的服务器不支持 STARTTLS，则消息将通常不使用 SSL 来投递。

选择证书

这个框显示你的 SSL 证书。单击此列表中的证书来指定它作为你希望邮件服务器使用的证书。双击一个证书来打开在证书

注意：
当前，MDaemon 对多个域不支持不同的证书。所有邮件域必须共享一个单独的证书。如果你有多于一个的域，之后输入那些域的名称到被称作“*多选择的主机名称（使用逗号分隔多个条目）*”中。

删除

选择列表中的证书，然后点击按钮删除它。确认框将打开并询问你，是否确定希望删除此证书。

创建证书

以下控制被用在创建证书中。编辑任何证书，双击它在以上列表中的它的条目。

主机名

输入你的用户将会连接的主机名称（例如，“mail.example.com”）。

组织/公司名

输入“拥有”证书的组织或者公司。

多选主机名（用逗号分开多条）

当前，MDaemon 对多个域不支持不同的证书 - 所有邮件域必须共享一个单独的证书。如果有你的用户可能连接到的主机名称以及你希望此证书也应用到那些名字，则输入在此输入那些域的名称，通过逗号分隔。由于允许通配符，因此“*.example.com”可以应用到所有 example.com 的下级域（比如，“wc.example.com”，“mail.example.com”，以及其他）。

密匙长度

为此证书选择希望的同步密匙的位长。同步密匙越长，数据传输就将会更安全。但是，注意：不是所有的应用程序都支持超过 512 的密匙长。

国家/地区

选择你的服务器存在的国家或者地区。

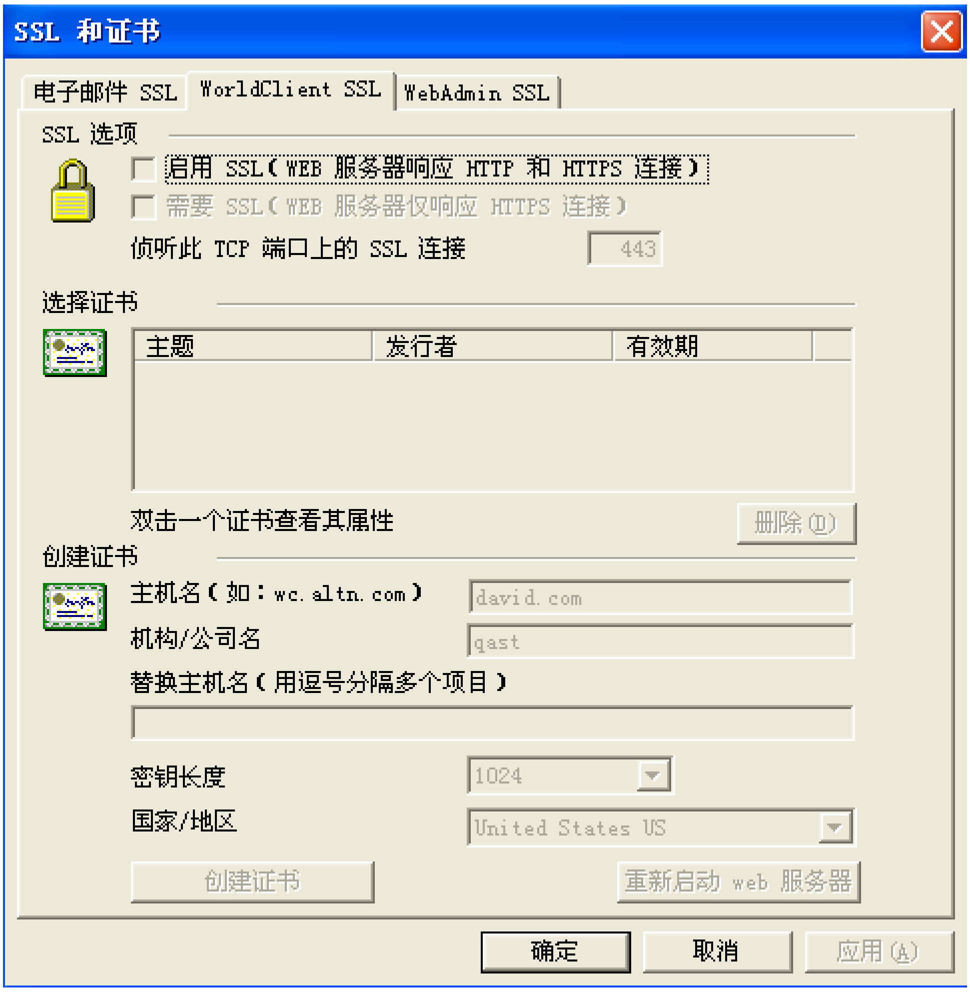
创建证书

在输入信息到以上控制中，点击此按钮创建你的证书。

重启服务

点击来重启 SMTP/IMAP/POP 服务。此服务必须在证书更改时重启。

WorldClient SSL



此选项是为了启用和配置 WorldClient 使用位于 SSL 和证书对话框上的 SSL 的（点击 Ctrl+L 或者安全 – SSL/TLS/证书… - WorldClient SSL）。为了你的便利，这些选项也在 WorldClient/RelayFax 属性对话框上（点击 Ctrl+W 或者设置 – WorldClient… - WorldClient SSL）。

注意：
这个对话框只有在使用 WorldClient 自己的内建 web 服务器时，才能使用。如果你已经配置 WorldClient 和 IIS 工作以提到它自己的 web 服务器，则这些选项将不能使用 – SSL 支持必须在 IIS 中配置。

SSL 选项

启用 SSL（web 服务响应 HTTP 和 HTTPS 连接）

如果你希望在 WorldClient 中启用 SSL 支持，点击此选项。但是这将不会强迫你的 WorldClient 用户使用 SSL。WorldClient 对在以下指定的 SSL 端口上的 HTTPS 连接进行监听，但是它仍将会回应在 Web 服务器标签上指定的 WorldClient 端口上的正常的 http 连接。

要求 SSL（web 服务仅回复 HTTPS 连接）

如果你希望在 WorldClient 中要求 SSL 支持，点击此检查框。当此选项启用时，WorldClient 将会只回应 HTTPS 连接 – 它将不会回应 HTTP 请求。

在此 TCP 端口上监听 SSL 连接

这次 WorldClient 将会为 SSL 连接监听的 TCP 端口。默认 SSL 端口是 443。如果默认端口被使用，则在通过 HTTPS 连接时，你将不能在 WorldClient 的 URL 中包含端口号（等同于 https://example.com 等于 https://example.com:443）。

注意：
这不同于在 web 服务器标签上指定的 WorldClient 端口。如果你仍允许 HTTP 连接到 WorldClient，则那些连接必须使用其他端口连接才能成功。HTTPS 连接必须为 SSL 端口。

选择证书

此选项显示你的 SSL 证书。单击在此列表中的一个证书来指定它作为你希望 WorldClient 使用的证书。在你能看到证书细节的证书对话框中，双击一个证书来打开它。

注意：
当前，MDaemon 对 WorldClient 不支持多个证书 - 所有 WorldClient 域必须共享一个单独的证书。如果你有多于一个 WorldClient 域，则输入那些域名称（以及其他你希望使用访问 WorldClient）到以下要点中称作“多选择的主机名称（使用逗号分隔多个条目）”中

删除

选择一个在此列表中的证书，然后点击此按钮删除它。一个确认框将会打开并询问你是否确定删除证书。

创建证书

下列控制用于创建证书。编辑任何证书，双击在上面的列表中的条目。

主机名

输入你的用户将会连接的主机名（例如，“wc.example.com”）。

组织/公司名

输入“拥有”证书的组织或者公司。

多选主机名（用逗号分开多条）

当前，MDaemon 不支持不同的证书 - 所有 WorldClient 域必须共享一个单独的证书。如果有你的用户可能连接到的另一个选择主机名称以及你希望此证书也应用到那些名字，则输入在此输入那些域的名称，通过逗号分隔。由于允许通配符，因此“*.example.com”可以应用到所有 example.com 的下级域（比如，“wc.example.com”，“mail.example.com”，以及其他）。

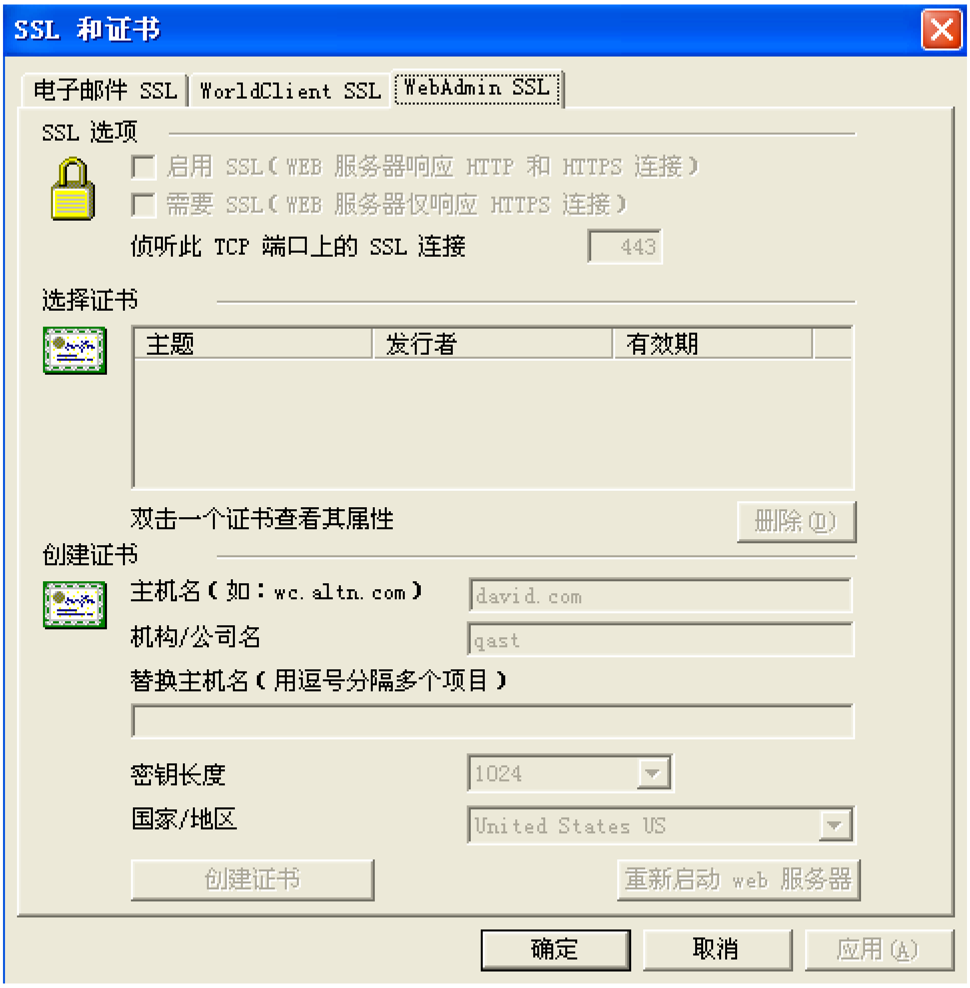
*密匙长度*为此证书选择希望的同步密匙的位长。同步密匙越长，数据传输就将会更安全。但是，注意：不是所有的应用程序都支持超过 512 的密匙长。

国家/地区
选择你的服务器存在的国家或者地区。

创建证书
在输入信息到以上控制中，点击此按钮创建你的证书。

重启 web 服务
点击来重启 web 服务。此服务必须在证书更改时重启。

WebAdmin SSL



此选项是为了启用和配置 WebAdmin 使用位于 SSL 和证书对话框上的 SSL 的(点击 Ctrl+L 或者安全 – SSL/TLS/证书… - WebAdmin SSL)。为了你的便利，这些选项也在 WebAdmin 对话框上（点击 Ctrl+W 或者设置 – WebAdmin… - WebAdmin SSL)。

注意：
这个对话框只有在使用 WebAdmin 自己的内建 web 服务器时，才能使用。如果你已经配置 WebAdmin 和 IIS 工作以提到它自己的 web 服务器，则这些选项将不能使用 – SSL 支持必须在 IIS 中配置。

SSL 选项

启用 SSL（web 服务响应 HTTP 和 HTTPS 连接）

如果你希望在 WorldClient 中启用 SSL 支持，点击此选项。但是这将不会强迫你的 WorldClient 用户使用 SSL。WorldClient 对在以下指定的 SSL 端口上的 HTTPS 连接进行监听，但是它仍将会回应在 Web 服务器标签上指定的 WorldClient 端口上的正常的 http 连接。

要求 SSL（web 服务仅响应 HTTPS 连接）

如果你希望在 WorldClient 中要求 SSL 支持，点击此检查框。当此选项启用时，WorldClient 将会只回应 HTTPS 连接 – 它将不会回应 HTTP 请求。

在此 TCP 端口监听 SSL 连接

这次 WorldClient 将会为 SSL 连接监听的 TCP 端口。默认 SSL 端口是 443。如果默认端口被使用，则在通过 HTTPS 连接时，你将不能在 WorldClient 的 URL 中包含端口号（等同于 https://example.com 等于 https://example.com:443）。

注意：
这不同于在 web 服务器标签上指定的 WorldClient 端口。如果你仍允许 HTTP 连接到 WorldClient，则那些连接必须使用其他端口连接才能成功。HTTPS 连接必须为 SSL 端口。

选择证书

此选项显示你的 SSL 证书。单击在此列表中的一个证书来指定它作为你希望 WorldClient 使用的证书。在你能看到证书细节的证书对话框中，双击一个证书来打开它。

注意：
当前，MDaemon 对 WorldClient 不支持多个证书 - 所有 WorldClient 域必须共享一个单独的证书。如果你有多于一个 WorldClient 域，则输入那些域名称（以及其他你希望使用访问 WorldClient）到以下要点中称作“多选择的主机名称（使用逗号分隔多个条目）”的控制。

删除

选择一个在此列表中的证书，然后点击此按钮删除它。一个确认框将会打开并询问你是否确定删除证书。

创建证书

下列控制用于创建证书。编辑任何证书，双击在上面的列表中的条目。

主机名

输入你的用户将会连接的主机名（例如，“wc.example.com”）。

组织/公司名

输入“拥有”证书的组织或者公司。

多选主机名（用逗号分开多条）

当前，MDaemon 不支持不同的证书 - 所有 WorldClient 域必须共享一个单独的证书。如果有你的用户可能连接到的另一个选择主机名称以及你希望此证书也应用到那些名字，则输入在此输入那些域的名称，通过逗号分隔。由于允许通配符，因此“*.example.com”可以应用到所有 example.com 的下级域（比如，“wc.example.com”，“mail.example.com”，以及其他）。

密匙长度
为此证书选择希望的同步密匙的位长。同步密匙越长，数据传输就将会更安全。但是，注意：不是所有的应用程序都支持超过 512 的密匙长。

国家/地区
选择你的服务器存在的国家或者地区。

创建证书
在输入信息到以上控制中，点击此按钮创建你的证书。

*重启 **web** 服务*
点击来重启 web 服务。此服务必须在证书更改时重启。

创建和使用SSL证书

在 Windows2000/XP 中，当使用 SSL 和证书对话框创建证书时，MDaemon 会生成自己签名的证书。换句话说，证书的发行者，或者证书权威（CA，和证书的拥有者是一样的。这是完全合法并被允许的，但是由于 CA 不会列入受信任的你的用户列表中，无论何时他们连接到 WorldClient 或者 WebAdmin 的 HTTPS URL，他们都将被问询是否他们希望继续访问站点并/或安装证书。在连接 WorldClient 或者 WebAdmin 时，一旦他们同意安全证书并且信任你的 WorldClient 的域作为一个合法的 CA，他们将不再必须看到安全警告消息。

但是，当通过邮件客户端，比如 Microsoft Outlook，连接 MDaemon 时，他们将不能给出安装证书的选项。他们允许选择是否他们希望继续使用临时证书，即使它没有被确认。每次他们开始他们的邮件客户端并连接服务器时，他们将不得不选择继续使用非确认证书。。为了避免此情况，你应该导出你的证书，并通过电子邮件或者其他方法分配它到你的用户。之后，他们可以手动安装并且信任你的证书，以避免未来报警消息。

在 Windows9x/Me/NT，你不能生成自签名证书。如果你正在使用这些处理系统之一，则 MDaemon 将会生成两个认证，一个为另外一个签名。第一个是为了服务器的域，另外一个（称作“MDaemon CA”）作为证书权威 – 域的证书将使得所列的 MDaemon CA 作为它的发行者。你将需要导出 MDaemon CA 证书并手动将其提供给你的用户安装（例如，通过电子邮件附件或者在你的网站上的下载连接）。更多情况下，双击一个*.cer 文件将会在你可以安装它的证书对话框中打开它。除非他们安装 MDaemon CA 证书，否则每次他们去你的 HTTPS URL 或者另外连接到你的邮件服务器，他们都将看到一个安全警告。

创建一个证书

从 MDaemon 中创建一个证书：

1. 移动到 MDaemon 中的 SSL 和证书对话框（点击 Ctrl+L 或者在 MDaemon 菜单栏上的安全 **– SSL/TLS/证书…** ）
2. 在所标的文本框中，“*主机名*”，输入证书属于的域（例如，“mail.example.com” ）。
3. 输入拥有证书的组织或者公司的名称到所标的文本框中，“组织/公司名”。
4. 在“可选主机名…”，输入所有你的用户将会用来访问你的服务器的其他域名（例如，“*.mydomain.com”，“example.com”，“wc.altn.com”，及其它）。
5. 从下拉列表框中，选择密匙长度。
6. 选择你服务器所在的国家/地区。
7. 点击创建认证书。

导出MDaemon CA证书

导出在 Windows 9x/Me/NT4 中的 MDaemon CA 证书：

1. 移动到 MDaemon 中的 SSL 和证书对话框（点击 Ctrl+L 或者 MDaemon 菜单栏上的 SSL/TLS/证书…）
2. 在证书对话框中，双击你的域的证书来查看它。
3. 打开证书路径标签。
4. 在证书对话框中，双击 MDaemon CA 证书来查看它。
5. 打开详细信息标签。
6. 点击复制到文件**…**
7. 点击下一步
8. 选择不，不要导出私钥，点击下一步
9. 选择 **DER** 编码**…**或者 **Base64** 编码**…**，点击下一步
10. 选择*.CER 文件和位置（等同于“C:\...\WorldClient\MDaemon_ca.CER”），点击下一步。
11. 点击完成。

使用由第三方CA发行的证书

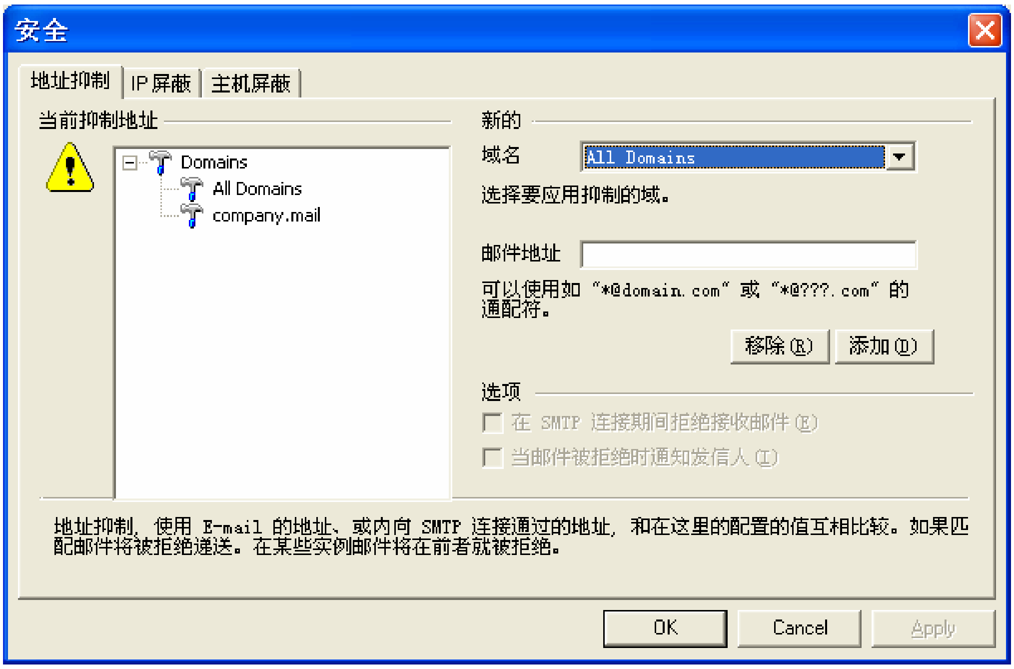
如果你购买或者从不是 MDaemon 的其他渠道另外生成证书，你仍通过使用 Microsoft 管理控制台导入到 MDaemon 使用的证书存储来继续使用那个证书。

1. 在你的 Windows 工具栏上，点击开始 **–** 运行**…**，然后键入“**mmc /a**”到“打开**:**”文本框。
2. 点击 **OK**。
3. 在 Microsoft 管理控制台中，点击文件 **–** 添加/删除管理单元**…**（或者按你键盘上的 **Ctrl+M**）。
4. 在独立标签上，点击添加**…**
5. 点击证书，然后点击添加
6. 选择计算机帐号，然后点击下一步
7. 选择本地计算机，然后点击完成

8. 点击**关闭**，然后点击**确定**
9. 在“证书（本地计算机）”下，如果你正在输入的证书是自署名的，那么点击在“受信任的根证书权威”文件夹下的“证书”下级文件夹。如果不是，则点击“个人”文件夹。
10. 点击**操作 – 所有任务 – 导入…**，然后点击**下一步**
11. 输入你希望导入的证书的路径（如果必要，使用浏览按钮），然后点击**下一步**。
12. 点击**下一步**，按后点击**完成**。

注意：
MDaemon 将只显示有使用个人信息交换格式（PKCS #12）的私人密匙的证书。如果你的导入的证书没有出现在列表中，则你可能需要导入*.PEM 文件，这个文件中包括证书密匙和私人密匙。使用与以上相同的处理过程概况导入此文件将会将其转化成 PKCS #12 格式。

地址抑制



使用安全 – 地址抑制…（或者 F4）来编辑在抑制列表上的地址。这个列表包括那些不被允许通过你的服务器发送邮件的地址。如果从此列表中的一个地址发来一封邮件，它将被接受并移动到坏消息队列或者在 SMTP 会话时拒收，并因此再不接受，这取决于你的设置。这对控制问题用户是非常有用的。地址可以基于每一个域或者整体的基础上被抑制（应用到所有 MDaemon 域）。

当前抑制地址

此窗口显示所有当前被域所抑制的地址列表。

新的

域名

选择此抑制地址将要应用的域。换句话说，你希望在什么域中从抑制地址阻止接收邮件？从此列表中选择“所有域”则会全面的抑制此地址。

注意：
从“所有域”类别中所列的地址发送的消息将会被接受然后被移动到坏消息队列。从指定域所列的地址发送的邮件将通过那个域的抑制设置进行操作。更多抑制选项，参看以下“*在 SMTP 连接期间拒绝接受邮件*”以及“*当邮件被拒绝时通知发信人*”。

邮件地址

输入你希望抑制的地址。由于接受通配符，因此*@badmail.com 将抑制所有来自“badmail.com”的消息，并且“frank@*”将会抑制所有名为“frank”的消息，无论消息是否从此域发出。

移除

点击此选项移除你在*当前抑制地址中显示*选择的条目。

添加
点击此按钮添加指定的用户到抑制列表中。

选项
*在 **SMTP** 连接期间拒绝接受邮件*
当启用此控制时，从抑制地址发送到选择的域的消息将会在 SMTP 处理阶段被拒绝。没有从抑制地址发送到选择域的邮件将会被存储到你的服务器，甚至在临时工作文件中。当此选项关闭时，邮件会被接受，但之后会被移动到坏消息队列。此功能是基于每一个域的；对“所有域”抑制地址是没有效果的。

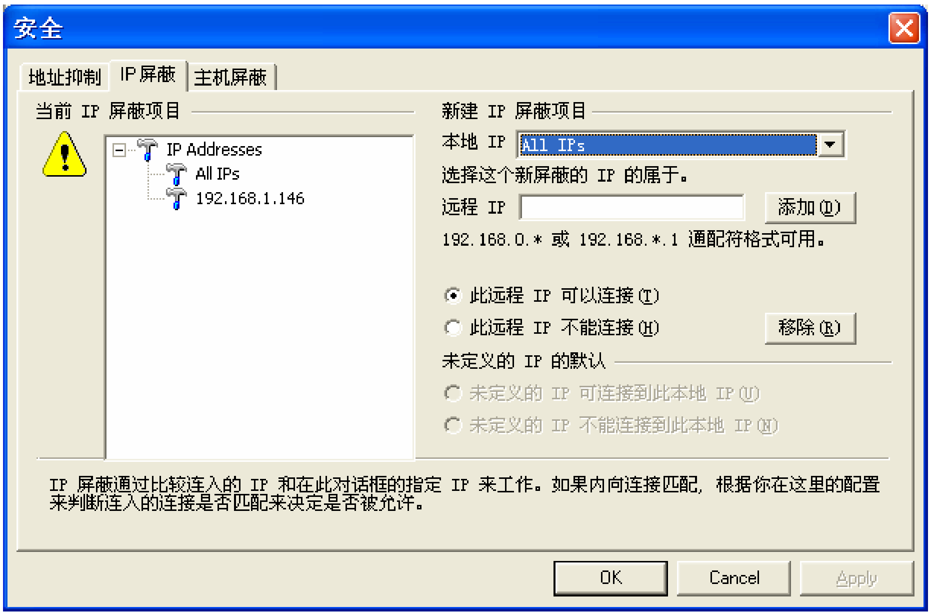
当邮件被拒绝时通知发信人
如果选择，一封客气的邮件将会被路由回受抑制的发送者，并告诉他/她，他们的邮件被删除了。这个功能是基于每一个域设置的。

注意：
为了此功能工作，邮件的复件必须在 SMTP 会话期间被下载下来，以便它能够被清除。从而，此选项与“*SMTP 会话期间拒绝接受邮件*”是矛盾的。

IP屏蔽

使用安全 – 地址抑制/ IP 屏蔽…（或者 F4）菜单部分来配置 IP 屏蔽。IP 屏蔽是一个你指定为可接收或者不可接收的 IP 地址的列表。服务器如何对待来自 IP 屏蔽上所列的 IP 地址的尝试连接，这取决于在屏蔽编辑器中选择的安全设置。你可能指定一个 IP 地址列表，然后配置服务器只接受在列表上的 IP 请求的连接，或者你可以配置它来放弃任何试图从此列表上的 IP 请求的连接。在任何四个 IP 地址位置中允许通配符。:

..*.*	匹配任何 IP 地址
206.*.*.*	匹配任何以 206 开头的 IP
206.97.*.239	匹配从 206.97.0.239 到 206.97.255.239 的 IP



当前 IP 屏蔽条目

此窗口显示所有 MDaemon 屏蔽的 IP 地址。他们是基于全局的或是基于本地 IP。

新建 IP 屏蔽条目

本地 IP

从下拉列表中选择“全部 IP”或者你希望应用屏蔽的本地 IP。

远程 IP

输入你希望添加到屏蔽列表的 IP 地址。你必须在小数点表格中输入此地址。这个 IP 屏蔽只能和 IP 地址工作。点击添加按钮添指定的 IP 地址到地址列表中。

此远程 IP 可以连接

选择此选项将会允许只有那些在指定域下的 IP 地址可以连接和发送邮件。没有在列表中列出的 IP 地址试图连接时将会被拒绝并立刻放弃。此选项对设置私人邮件网络系统是非常有用的。

此远程地址不能连接

选择此选项将允许所有那些没有在地址列表中的 IP 地址连接并发送消息。从地

址列表中指定的 IP 地址试图连接将会被拒绝并被立刻放弃。此选项对于你的邮件系统排除会导致邮件系统产生问题的 IP 地址是非常有用的。

添加

点击此选项，在 *IP 地址控制*中添加指定的地址到*当前 IP 屏蔽设置*窗口。

移除

点击此选项从列表中移除一个选择的条目。

未定义的 **IP** 的默认值

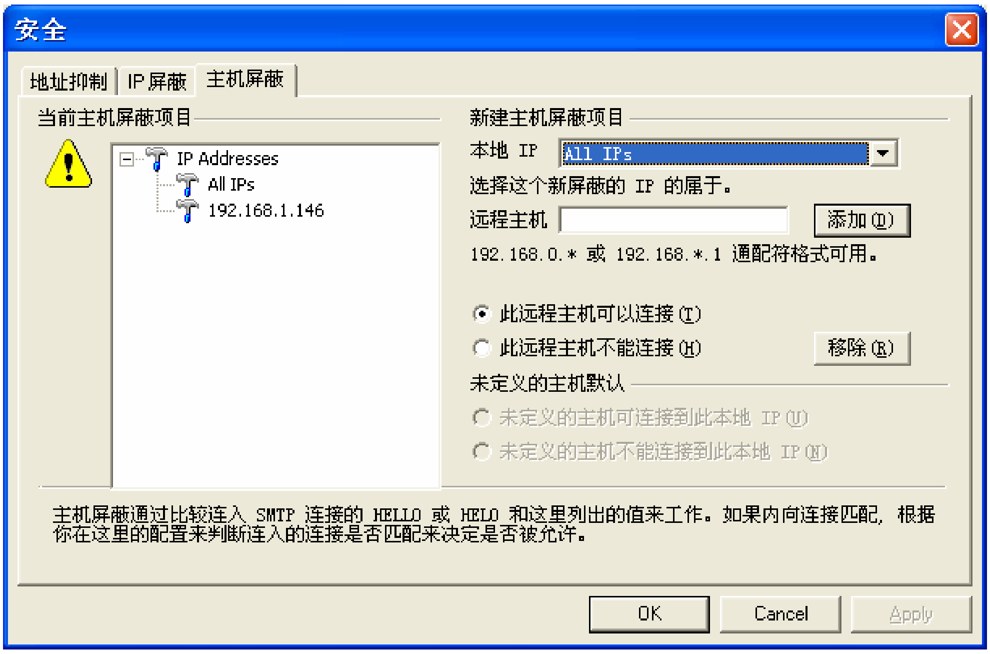
未定义的 IP 可连接到此本地 IP

当此选项被选择时，所有没有在 IP 屏蔽中的 IP 地址将被允许连接。

未定义的 IP 不能连接到此本地 IP

当此选项被选择时，只有在 IP 屏蔽中特别授予权限的 IP 地址才允许连接。

主机屏蔽



当前主机屏蔽条目

此窗口显示所有 MDaemon 屏蔽的主机。他们是基于全局的或是基于本地 IP。

新建主机屏蔽项目

<u>本地 IP</u>

从下拉列表中选择“全部 IP”或者你希望应用屏蔽的本地 IP。这是远程主机试图连接的 IP 地址。

<u>远程主机</u>

输入你希望添加到屏蔽列表的主机。由于允许通配符，因此你可以输入“*.example.com”来阻止或者允许所有来自 example.com 的下级域的连接，或者“example.*”，来对所有以“example.”开头的顶级域进行屏蔽。点击添加按钮添指定的主机到地址列表中。

<u>此远程主机可以连接</u>

选择此选项将会允许只有那些在给定的域下指定主机才能连接和发送主机。没有在列表中指定的主机试图连接将会被拒绝并立刻放弃。此选项对设置私人邮件网络系统是非常有用的。

<u>此远程地址不能连接</u>

选择此选项将允许所有那些不是在地址列表中指定的主机连接并发送消息。从地址列表中指定的主机试图连接将会被拒绝并被立刻放弃。此选项对于你的邮件传输系统排除在外的，并对产生问题的主机是非常有用的。

<u>添加</u>

点击此选项添加主机到列表。

移除

点击此选项从列表中移除一个选择的条目。

未定义的主机默认

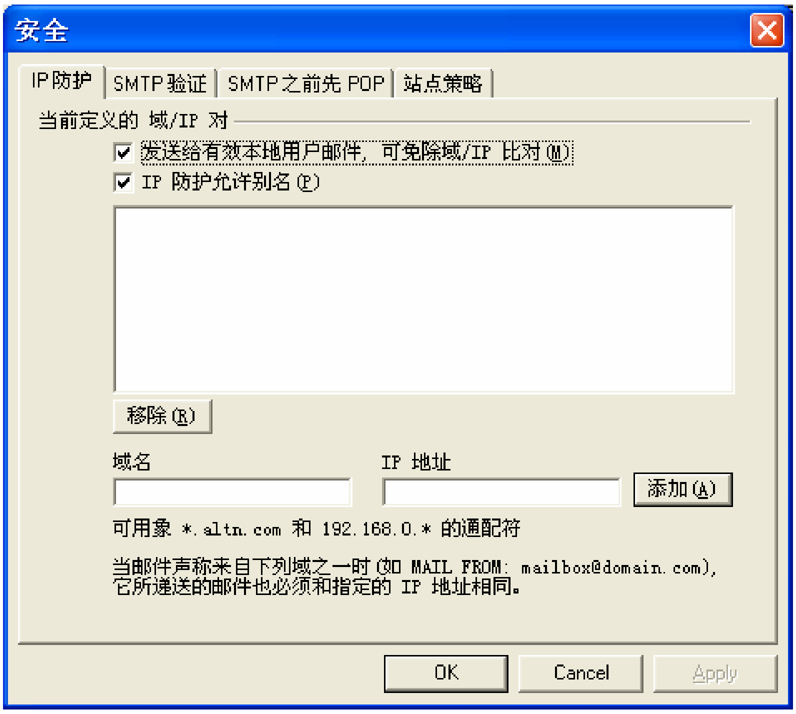
*未定义的主机可连接到此本地 **IP***

当此选项被选择时，所有没有在主机屏蔽中的主机将被允许连接到指定 IP 地址。

*未定义的主机不能连接到此本地 **IP***

当此选项被选择时，只有在主机屏蔽中特别授予权限的主机才允许连接到指定 IP 地址。

IP防护



使用安全 – IP 防护…菜单部分来配置 IP 防护。IP 防护是域名称和在 SMTP MAIL FROM：命令中被检查的匹配的 IP 地址的列表。当一个 SMTP 连接声称来自域名列表上时并且他的 IP 地址在关联 IP 列表中，此会话才被接受。例如，假设你的域名为 MDaemon.com，你本地 LAN 计算机使用范围从 192.168.0.0 到 192.168.0.255 的 IP 地址。根据此信息，你可以设置 IP 防护与域名为 MDaemon.com，IP 地址范围为 192.168.0.*相关连（允许通配符）。因此任何时候，一台计算机连接到你的 SMTP 服务器，并表述，“MAIL FROM someone@MDaemon.com”，SMTP 会话只有在连接的计算机拥有要求范围是 192.168.0.1 到 192.168.0.255 中的某一 IP 时将会接受。

当前定义的域/IP 对

这是域名称和在某一个 IP 试图连接 MDaemon 时，被用来比较的关联 IP 地址列表。

发送给有效本地用户邮件，可免除域/IP 匹配

如果你希望只有那些目标为非本地用户或者不合法本地用户的消息被域/IP 匹配检查，点击此选项。这将阻止那些伴装为你本地用户的其他人来通过你的服务器转发邮件，而不会在不检查那些发送邮件到你服务器上的用户情况下保存邮件。

IP 防护允许别名

在点击域/IP 地址防护时，如果你希望 IP 防护允许地址别名，点击此选项。如果点选了 *IP 防护允许别名*，IP 防护将会转发一个别名到它所指向的真实帐号，并因此在其通过了防护情况下，允许它。没有启用此选项，IP 防护将会把每一个别名当作它所显示的帐号的独立地址。因此，如果一个别名的 IP 地址违反 IP 防

护，则邮件将被拒绝。此选项是别名编辑器的镜像（帐号 – 地址别名…）- 在此改变设置将会在那边反映出来。

如果你希望到合法地址别名的来信能够被 IP 防护免除，则点击此选项和*发送给有效本地用户邮件，可免除域/IP 比对*选项。

域名

输入你希望关连到你指定 IP 地址范围的域名称

IP 地址

输入你希望与一个域名称相关连的 IP 地址。你必须在小数点格式中输入此地址。

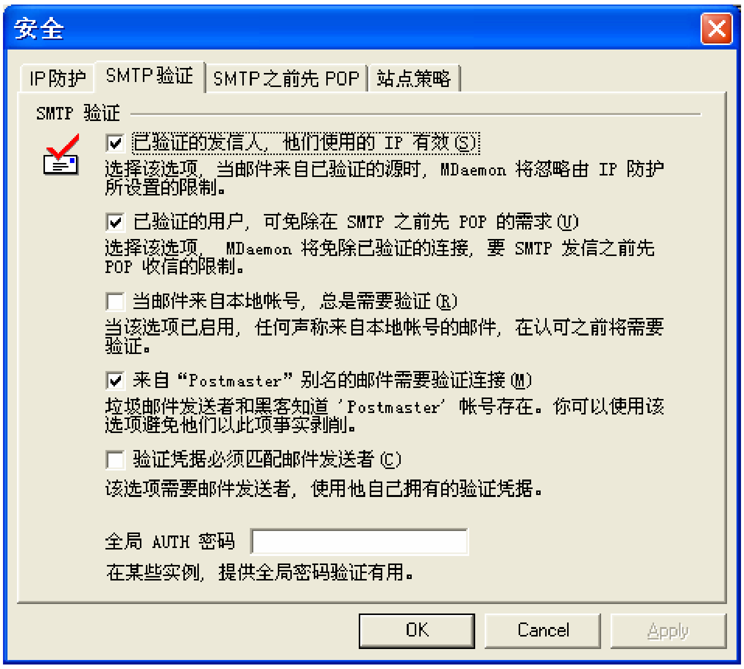
添加

点击添加选项添加域和 IP 地址范围到列表。

移除

点击此按钮从列表中移除选定的条目。

SMTP认证



SMTP 验证

已验证的发信人，他们使用的 IP 有效

当此控制开启时，当前防护的 IP 地址将不能应用到已经被认证的用户。无论他们从什么样的 IP 地址发送，邮件都将被接受。

已验证的用户，可免除在 SMTP 之前先 POP 的需求

如果你在 SMTP 安全功能前，利用 POP，你应该点击此控制来使得认证用户从此限制中免除。一个认证用户在发送消息前，将不需要检查他或她的电子邮件。

当邮件来自本地帐号，总是需要验证

如果个人发送一个宣布来自 MDaemon 域之一的邮件，账户必须首先被认证否则 MDaemon 将会拒绝接受邮件发送。

注意：
激活此选项意味着发件人和收件人双方都需要认证。如果你想让均为本地的发件人和收件人在此要求中免除，那么你可以通过编辑在 MDaemon.ini 文件中的以下设定来实现： [Special] ForceAUTHExemptLocal=Yes（default No） 这对于某些你需要你的用户对来信和发信使用不同的邮件服务器的情况是非常必要的。

来自 ‘Postmaster’ 别名的邮件需要验证连接

点击此复选框要求在 MDaemon 接受声明来自 postmaster@...别名之一的邮件被认证。垃圾邮件发送者和黑客知道“postmaster”存在并试图使用此帐号通过你的系统发送邮件。此选项将会阻止他们和其他未认证的用户这么做。此选项在别名编辑器上也可用（帐号 – 地址别名…）。在此改变此设置将会在那里反映出来。

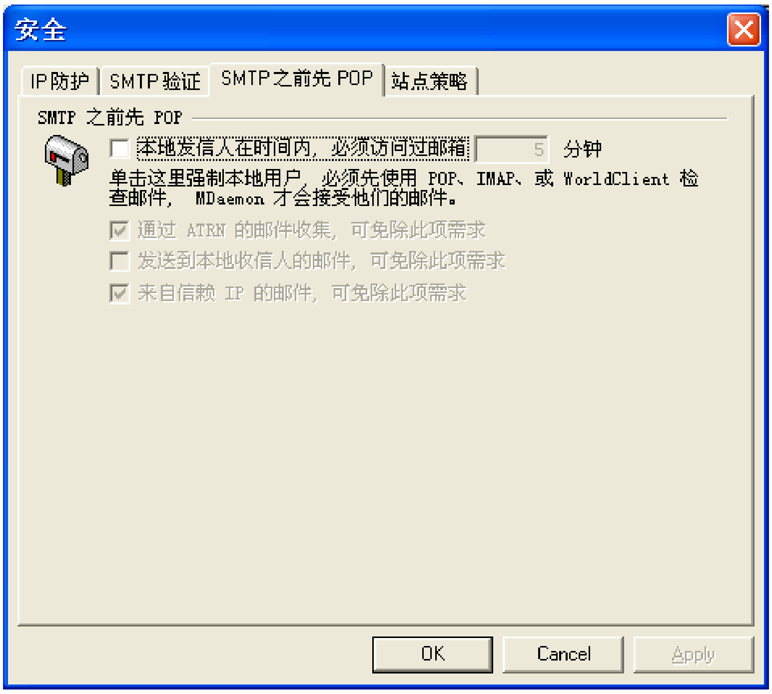
验证凭据必须匹配邮件发送者

如果你希望要求那些在 SMTP 投递期间认证的用户只使用他们自己的认证证书，点击此复选框。登录和使用的密码必须是那些在 SMTP MAIL 命令中发件人给定的。这将阻止合法本地用户从不是他们自己的地址通过你的系统发送电子邮件。

全局 AUTH 密码

如果*无论认证发送者使用此 IP，他们均为合法*选项启用，配置为动态 NT 认证 MDaemon 帐号必须为认证使用此全局 AUTH 密码以代替他们通常的 NT 密码。

SMTP之前先POP



SMTP 之前先 POP

本地发信人必须访问过邮箱 xx 分钟内

在此功能启用时，无论何时某一个 IP 声明作为一个本地用户，在他们被允许发送邮件前，他们都必须登录并且在指定的时间内检查他们的本地邮箱。

通过 ATRN 的邮件收集，可免除此项需求

如果你希望通过 ATRN 收集的邮件在 SMTP 要求前可以从 POP 中免除，点击此选项。

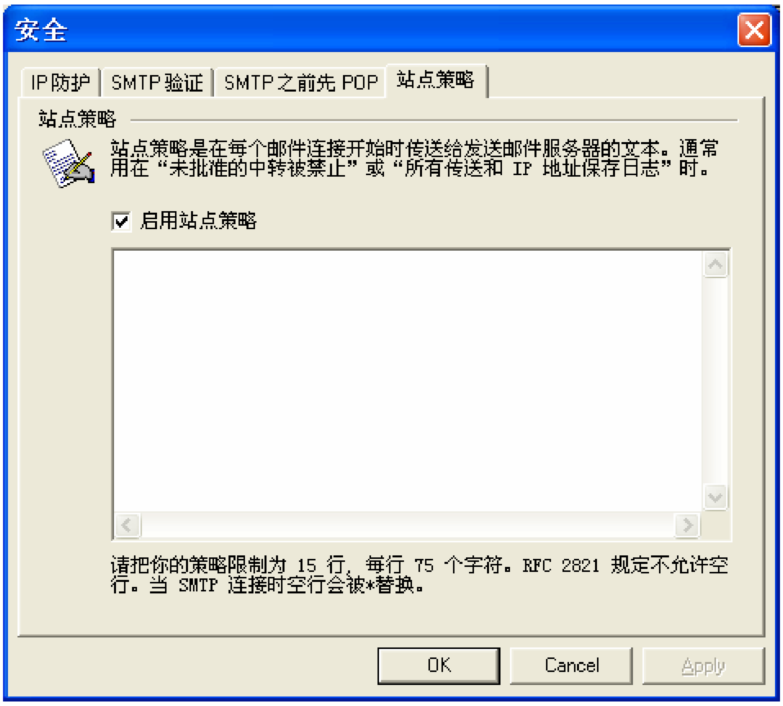
发送到本地收信人的邮件，可免除此项需求

如果你希望从一个本地用户发送到另一个本地用户的邮件可以在"*本地发信人在时间内...*"要求中免除，点击此选项。通常，一旦知道了发件人，MDaemon 将会强制执行"在 SMTP 之前 POP"要求，但是当此控制启用时，MDaemon 将会在决定它是否需要前一直等待，直到显示消息的收件人。

来自信赖 IP 的邮件，可免除此项需求

如果此复选框启用，来自此话框的当前定义的域/IP 区域中所列的域的邮件将从*本地发信人在时间内...*要求中免除。

站点策略



创建一个SMTP连接策略声明

使用此对话框指定站点安全政策。在位于 MDaemon 的\app\下级文件夹中的 policy.dat 文件中存储的文本被用来在每一个 SMTP 邮件会话的开头传输发送到服务器。一个普通站点政策的例子是，"This server does not relay"或者"Unauthorized use prohibited"。你不需要预先计划每一行使用"220"或者"220-"。在有或者没有这些预设的代码的情况下，Mdaemon 都会每一行进行操作，。

一个站点使用的政策就关于转发邮件的声明在 SMTP 处理期间可以像这样：

220-Alt-N Technologies ESMTP MDaemon v8.0

220-This site does relay unauthorized email.

220-If you are not an authorized user of our server

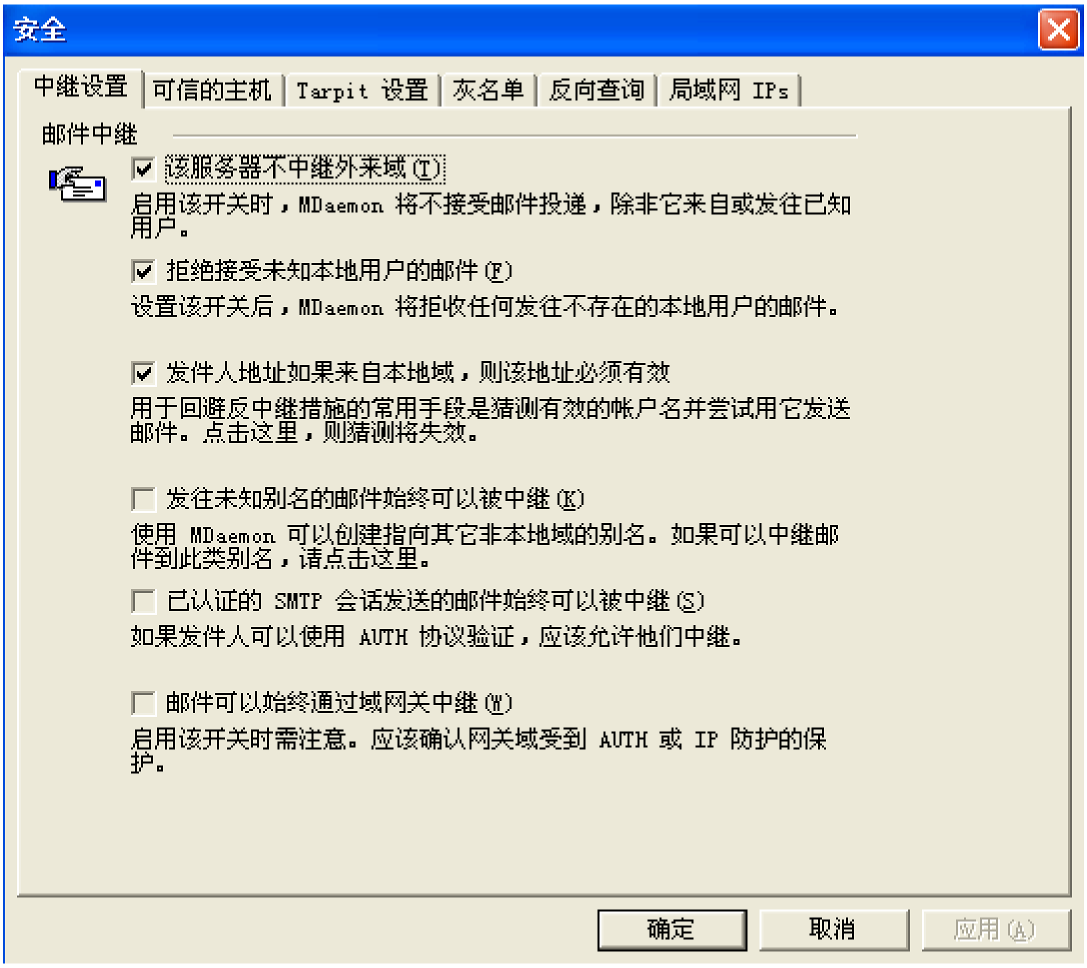
220-then you must not relay mail through this site.

220

HELO domain.com…

POLICY.DAT 文件必须只由可打印的 ASCII 文本组成，并且每行不超过 512 个字母；但是强烈推荐每行不超过 75 个字母。此文件的最大容量为 5000 字节。在超过 5000 字节时，MDaemon 将不会显示文件。

中继设置



使用安全 – 中继/…（Alt+F1）菜单部分来定义你的服务器如何回应邮件转发。当一封到达你的邮件服务器的邮件既不是来自也不是发送到本地地址，你的服务器会被要求未知的第三方转发（或者投递）邮件。如果你不希望你的服务器为未知用户转发邮件，你可以使用在此提供的选项。

警告：
对其他服务器不加以选择的转发邮件可能导致在你的域成为一个或者多个 RBL 主机的黑名单（参看 127 页）。开放的转发是极不鼓励的，这是因为“垃圾邮件发送者”使用开放服务器来隐藏他们的踪迹。

邮件中继

此服务器不中继外来域的邮件

当选择了此开关时，MDaemon 将拒绝接收来自和发送都不是非本地用户的投递邮件。

拒绝接收给未知本地用户的邮件

当此复选框启用时，MDaemon 将拒绝接受对本地域但地址为不存在用户的邮件。

“本地”包括 LAN 和域网关。

如果发送者声称来自本地域，则他的地址必须可用

如果个人发送一封来自 MDaemon 的域之一的消息，使用的帐号被帐号数据库校验。本地帐号必须存在或者 MDaemon 将拒绝接受邮件。

到已知别名地址的邮件可以总是被中继

如果你希望 MDaemon 为地址别名转发邮件（331 页），无论你的转发控制设置如何，点击此选项。

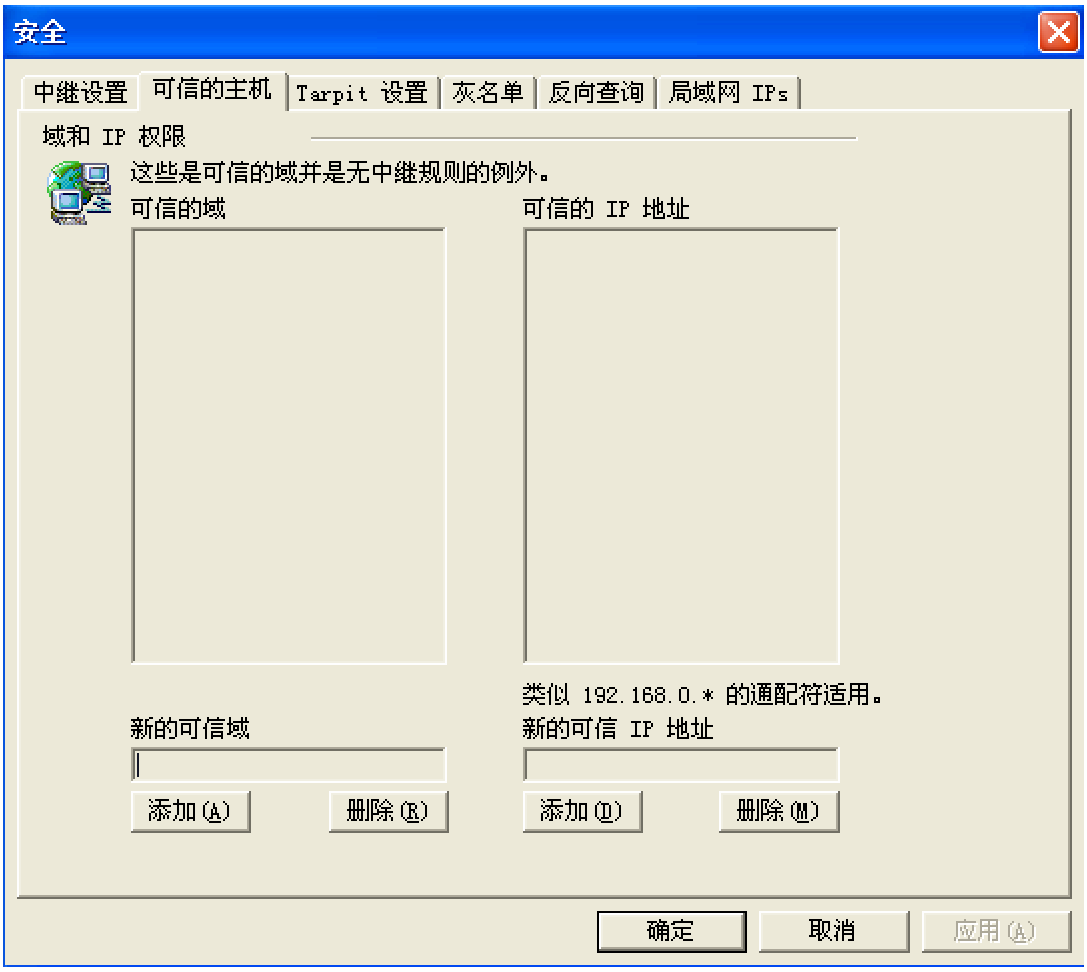
*通过认证 **SMTP** 连接发送的邮件总是可以被中继*

当此复选框启用，在通过认证的 SMTP 会话发送邮件时，MDaemon 将会转发邮件。

邮件可以通过域网关总是被中继

如果你希望 MDaemon 允许邮件通过域网关转发，无论你的转发设置如何，启用此复选框。此功能默认情况下为关闭并且不推荐使用。

可信的主机



域和 **IP** 允许

可信的域

在此所列的域是转发规则的例外。这些域被你的服务器“所信任的”，并且 MDaemon 将会为他们的用户转发邮件。

新的可信域

输入一个新的域名称添加到*受信任域*列表。

添加

点击此按钮添加新的域到受信任的域列表。

移除

点击此按钮从受信任域列表中移除所选的条目。

*可信的 **IP** 地址*

在此所列的 IP 地址是转发规则的例外。这些 IP 地址被你的服务器“所信任的”，并且 MDaemon 将会为他们的用户转发邮件。

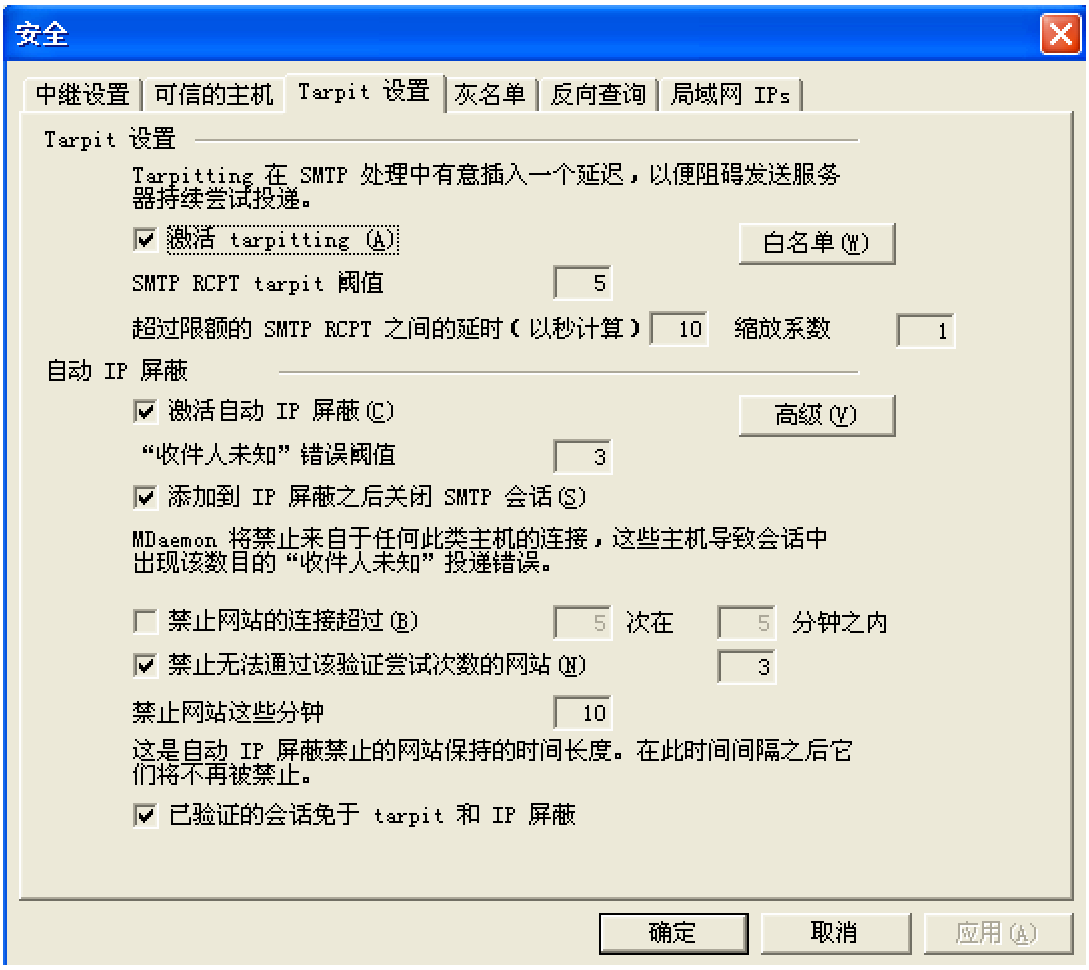
*新的可信 **IP** 地址*

输入一个新的 IP 地址名称添加到*受信任 IP 地址*列表。

添加
点击词按钮添加新的 IP 地址到受信任的 IP 地址列表。

移除
点击此按钮从受信任 IP 地址列表中移除所选的条目。

Tarpit 设置



点击安全 – 中继/可信的/Tarpit/…（Alt+F1）打开此对话框。它用来配置两个安全功能：Tarpitting 和自动 IP 屏蔽。

一旦从一个从邮件发送者接收到指定数量的 RCPT 命令，Tarpitting 使得你有意的减慢一个连接成为可能。这将阻碍垃圾邮件发送者尝试使用你的服务器发送未请求的垃圾邮件。你可以指定在开始 tarpitting 前允许的 RCPT 命令数量以及在连接期间从主机接收到的命令之间延迟的时间。在此技术下的假设是如果使得垃圾邮件发送者每发送一个邮件都花费很长时间，则将使他们不会在未来使用你的服务器再次尝试这么做。

如果在邮件会话中，从某个地址发过来一定数量的“收件人未知”错误，那么这个地址将会被自动 IP 屏蔽阻止再次连接到 Mdaemon。你也可以阻止试图通过你邮件服务器中转或发送未知本地帐号的主机。这些 IP 地址和主机不会被永久的阻止，只会屏蔽在设定中设定的时间。Tarpit.dat 文件包括一个 IP 地址列表以及他们被阻止了多长时间。这个文件长驻内存，可以手工编辑。还可以创建一个空白文件 Tarpit.sem 放在 Mdaemon\App\文件夹。使得 Mdaemon 重新加载长驻内存的 Tarpit.dat 文件从而使你的改变生效。

阻止设置

激活阻止

点击这个选项来激活 Mdaemon 阻止设置。

SMTP RCPT tarpit 阀值

在 Mdaemon 开始阻止主机之前，你允许在一个会话中这个主机能发送 RCPT 命令的数量。列如：如果这个数量设成 10，而发送主机试图发送一封邮件到 20 个地址（20 个 RCPT 命令），然后 Mdaemon 将允许最初的 10 个而暂停以后每个命令一段时间，这个时间就是在 ***SMTP RCPT tarpit 延时***中设定的数值。

SMTP RCPT tarpit 延时

一旦一个主机到达 ***SMTP RCPT tarpit 阀值***，这个时间就是暂停以后每个命令的时间数值。

缩放系数

这个数值是被用来作为基本 tarpit 延时增加的乘法系数。tarpit 阀值到达以后，那 tarpit 延时就会作用到此会话上，每一个延时会乘以这个系数来决定在这个会话中下个延时的长度。例如：如果 tarpit 延时设成 10 而缩放系数是 1.5，那么第一个延时将是 10 秒钟，第二个延时是 15 秒，第三个延时是 33.75 秒，等等。默认的缩放系数是 1，意味着延时将不会增加。

白名单列表

点击这个按钮，打开 Tarpit 白名单列表对话框。在此你可以指定哪些 IP 地址将免除 Tarpit。

自动 **IP** 屏蔽

*激活自动 **IP** 屏蔽*

点击这个复选框激活自动 IP 屏蔽。

高级

点击这个按钮用记事本打开tarpit.dat文件。这个文件列举了所有被自动IP屏蔽所阻止的IP地址。你可以手动的添加IP地址和延时的时间。在列表中每一行添加一个条目，`IP_address<space>Minutes` 如`1.2.3.4 60`。

"收件人未知"错误阀值

在 Mdaemon 开始阻止主机之前，你允许在一个会话中这个主机能发送收件人未知命令的数量。经常的"收件人未知"错误通常是垃圾邮件发送者试图发送到过期的或错误地址的一个线索。

*在添加到 **IP** 屏蔽后关闭 **SMTP** 会话*

开启这个选项使得 Mdaemon 在把由于到达"未知收件人"阀值的 IP 地址加入到 IP 屏蔽后，关闭 SMTP 连接。这个选项默认是打开的。

*禁止站点的连接超过**[X]**次**[X]**分钟*

点击这个复选框如果你希望临时的禁止那些在限定的时间内超过连接次数的服

务器。指定在多长时间内允许连接的次数。

禁止站点认证尝试失败次数

使用这个选项，如果你希望临时禁止那些认证尝试次数达到或超过设定的数值。这将帮助你阻止一个用户帐号被入侵。

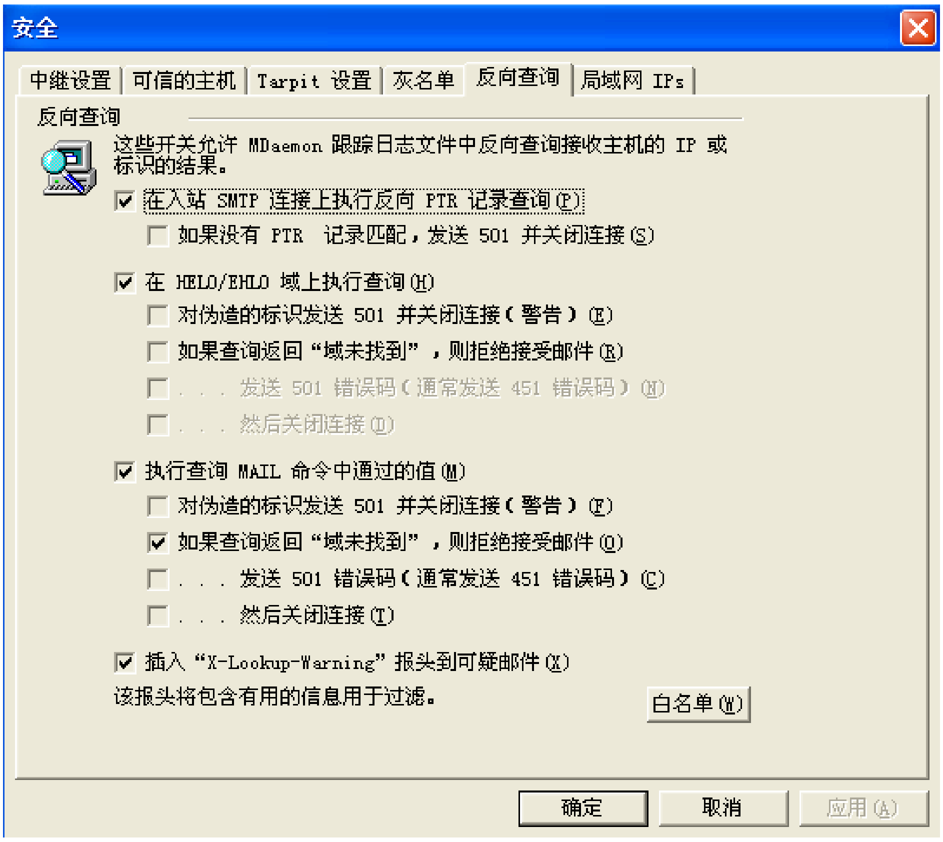
禁止站点这些时间

当一个 IP 被自动禁止后，将会禁止这些时间。当过了这个禁止时间后，这个 IP 才会正常的收发邮件。这个功能将确保你不会永久的禁止一个合法的 IP。

认证的用户将免除 Tarpit 和 IP 屏蔽

点机这个选项如果你希望你的认证的用户免除 Tarpit 和 IP 屏蔽

反向查询



使用这个功能，Mdaemon可以反向查询在the `HELO/EHLO` 或`MAIL`中传递的命令。当执行反向查询时，Mdaemon将尝试获取指定域名的所有的MX和A记录。然后，对方服务器连接上来的IP地址将会用来和查询到的记录进行匹配来决定发信者是否是伪造的。

通常发信服务器的IP地址，将不会匹配任何指定域名已知的MX和A记录，而可以仍然正常的传递邮件。反向查询的主要目的不是拒绝邮件，而是尽可能多的将信息记录到日志中去，然后提供给管理员根据自己的本地安全策略来处理这些邮件。最后，如果没有通过反向查询的邮件在邮件头中会插入一个特定的邮件头。内容过滤器会决定包含这些邮件头的邮件的命运。

你还可以执行对于PTR记录的查询，当使用这个选项的时候，如果连接进来的IP地址没有任何匹配的PTR记录，那么这个连接将会被放弃或在邮件头中插入一个警告信息。

最后，是不是接受一个并不存在的域名发过来的邮件是可选的。因此，有选项来设置服务器可以拒绝一封在反向查询中返回域名未知的邮件。在这种情况下，Mdaemon将返回451错误代码，拒绝接收邮件，。然而如果你希望立即断开连接并返回501错误代码，服务器将会有另外的选项来达到此目的。

可信任的IP地址和本地地址（127.0.0.1）总是免除反向查询。

反向查询

对入站的SMTP连接执行反向的PTR记录查找

启用这个选项如果你希望Mdaemon对于入站的SMTP连接执行反向的PTR记录查找。

…如果没有匹配PTR记录，发送501然后关闭连接

如果这个复选框被选中，Mdaemon将发送501错误代码。

对HELO/EHLO域名执行查询

选中此项，如果你希望对连接中对方服务器报告的HELO/EHLO域名进行反向查询。HELO/EHLO命令是发送服务器端发送来标识自己的。在这个命令中传递的域名被服务器写入邮件的from部分的Received邮件头中。

执行查询MAIL命令中传递的值

启用这个选项执行对于在邮件连接中MAIL命令传递的域名反向查询。在MAIL命令中传递的地址应该对于邮件是可追溯的，通常是邮件的来源的邮箱。

…对于伪造的标识，发送501然后关闭连接（谨慎）

选中这个复选框，如果反向查询的结果显示是一个伪造的标识，Mdaemon将发送501错误代码然后关闭连接。

谨慎！

当反向查询的结果显示如果服务器好象使用了一个伪造的标识，这个结果很有能是错误的。通常邮件服务器不一定用和IP地址匹配的域名标识自己。这可能是ISP的限制和约束或其他合法的原因。由于这样，你必须谨慎的开启这个选项。很有可能，这个选项会导致一些正常的邮件被拒收。

如果查询返回"域名没找到"，则拒绝接收邮件

如果查询返回"域名没找到"的结果，开启这个选项到导致邮件被拒收并返回451错误代码而连接可以正常的结束。

…发送501错误代码（通常发送451错误代码）

点击这个复选框，如果你想发送"域名未找到"结果响应错误代码为501而不是451。

…然后结束连接

点击这个复选框，如果你想反向查找结果返回"域名未找到"时立即结束连接

在可疑的邮件中插入"X-Lookup-Warning"邮件头

点击这个复选框，如果你想在反向查询结果显示可疑的邮件中插入邮件头。你可以在Mdaemon.ini编辑邮件头的名字和内容：

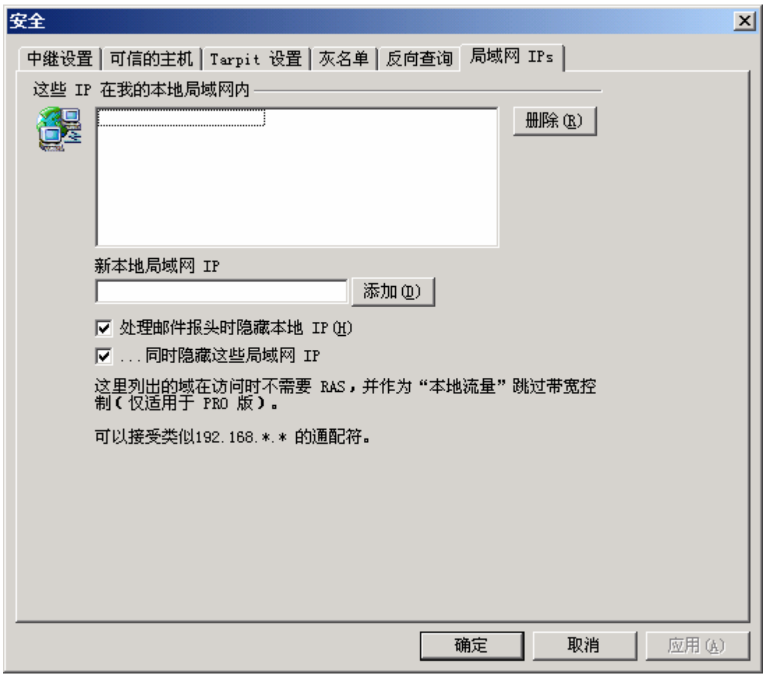
```
[Special]
LookupWarningHeader=X-LookupWarning: text
```

如果你编辑这个值，Mdaemon允许你“X-LookupWarning: text”为任何你想要写的内容。但是要确保你的更改必须要符合邮件头的RFC规范。

白名单列表

点击这个按钮打开反向查询白名单列表对话框，你可以在这里指定要免除反向查询的IP地址。

局域网 IPs



注意:这个对话框等同于的RAS拨号设置和带宽限制的相同位置。在此设置的改变将会应用到所有的位置。

这些地址在我的本地局域网内

这个标签用来列举你的本地局域网的IP地址。因此这些IP地址将不需要RAS来访问他们，而且他们也被当作本地通讯而不受带宽限制设定的约束。因为他们是本地地址，所以他们将免除还有很多其他的安全和防垃圾的选项的限制。

移除

在列表中选择一个IP地址，然后按这个按钮来移除。你也可以双击一个条目来移除它。

新建本地局域网IP

输入一个IP地址然后按*添加*加入到IP地址列表。如127.0.*.*是允许的。

添加

在*新建本地局域网IP*中输入一个IP地址后，按这个按钮来添加。

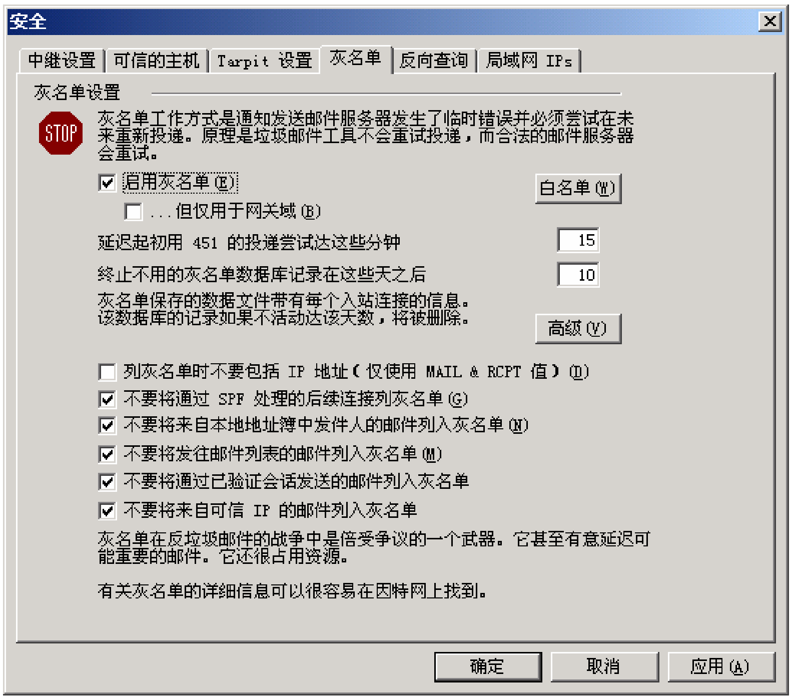
处理邮件头时隐藏本地IP地址

启用这个选项如果你希望Mdaemon在创建received邮件头时隐藏所有本地IP。

…也隐藏这些局域网IP

如果Mdaemon配置成隐藏本地IP地址，而且也想隐藏这些局域网IP就选中这个复选框。

灰名单



从安全对话框中进行配置(位于Security Relay/…/Greylist… Greylisting)，灰名单是一项反垃圾邮件技术，它利用了SMTP服务器重新发送任何收到临时出错代码（如“稍后再试”）的邮件信息。通过这项技术，当一个邮件从一个非白名单列表或先前未知的发件人到达服务器时，在SMTP进程中它会被灰名单拒绝并收到一个临时出错代码。而且，在一段指定的时间内（如，30分钟），任何重新发送的企图将被临时拒绝。 因为垃圾邮件发送者在邮件被拒绝后通常不会重新发送。灰名单能帮助显著减少你的用户收到垃圾邮件的数量。即使垃圾邮件发送者企图在后来重新发送邮件，很可能那时垃圾邮件发送者已经被成功识别并且被其它反垃圾邮件选项(如，DNS黑名单)成功地阻止。值得注意的是，这项技术也会同时延缓某些正常邮件的接收。但是，合法邮件还是会在定义的灰名单时间段失效后被重新发送。还有一点需要注意的是，在作进一步发送尝试之前你没有办法得知发送服务器将等待多久。故意拒绝一个带有临时错误代码的邮件可能会引起这个邮件被延迟发送，少则数分钟，也可能长达一整天。

灰名单会产生几个常见的问题和负面作用，灰名单对话框包含许多选项来应对这些问题。首先，一些发件域使用一个邮件服务器集合来对外发送邮件。不同的邮件服务器可以被用作每一次的发送尝试，每次尝试将被作为一次全新的连接到灰名单引擎。这会让邮件通过灰名单的时间成倍增加，因为每一次的尝试都将被当作单独的邮件而不是原先邮件的重试进行灰名单验证。通过使用一个SPF查找选项，这个问题对于那些发布其SPF数据的发件域可以被解决。而且，有一个选项可以用来完全忽略发件服务器的IP地址。使用这个选项降低了灰名单的效能，但是这可以完全解决服务器集合的问题。其次，由于每个进入的连接都必须被追踪，灰名单通常承担着一个巨大的数据库。MDaemon通过将灰名单功能放置在SMTP处理进程的几乎是最后部分来追踪连接，以实现开销最小化。这使得所有

MDaemon的其它选项在邮件到达灰名单阶段前先根据各自规则拒绝部分邮件。因此，灰名单数据文件的大小被显著地减小了，而且它是驻留内存的，对实际性能的影响很小。最后，几个选项可以被用来减小灰名单对正常邮件的影响。首先，被发送到邮件列表的邮件可以被排除在外。其次，灰名单有自己的白名单文件，你可以从中指定IP地址，发件人和收件人被免于灰名单验证。最后，灰名单包含了一个选项用于将每个帐号的私人地址簿文件作为一个白名单数据库。这样，从用户地址簿中某人发给该用户的邮件可以被免于灰名单验证。
更多关于灰名单的信息，请访问Even Harris的网站：
http://projects.puremagic.com/greylisting/.

灰名单设置

启用灰名单
点击这个选项来启用MDaemon中的灰名单功能。

…但是仅对于网关域
点击这个复选框，如果你只想对发往网关域的邮件应用灰名单。

白名单
这个按钮打开了灰名单自己的白名单，从中你可以指定哪些发件人，收件人和IP地址可以被免于灰名单验证。

*延迟初始发送尝试这些分钟并返回**451***
指定对初始尝试后的发送尝试进行灰名单验证的分钟数。在这段时间内，任何后来的来自同一个服务器/发件人/收件人组合的发送尝试将被拒绝并给出另一个临时错误代码。当灰名单时间过去后，对那个三个一组的组合不会有进一步的灰名单延迟将被执行，除非灰名单数据库记录已经过期。

在这些天数之后未使用的灰名单数据库记录过期
对于一个给定的灰名单组合，在初始的灰名单时期失效后，匹配那个组合的邮件将不会被灰名单延迟。然而，在这个选项中指定的天数内，如果没有接收到匹配那个组合的邮件，它的灰名单数据库记录将会过期。后来的由那个组合发出的尝试将会导致创建一个新的灰名单记录，它将不得不再次等待初始的灰名单规定的时间。

高级
点击这个按钮来打开灰名单数据库，你可以使用它来浏览或编辑你的灰名单数据库。

*在灰名单验证时不要包含**IP**地址**(**仅使用**MAIL & RCPT**值**)***
点击这个复选框，如果你不想使用发件服务器的IP地址作为灰名单参数之一。这将解决可能由服务器集合引起的潜在问题，但这也会降低灰名单的效能。

<u>不要对通过SPF处理的后来的连接进行灰名单验证</u>
当使用这个选项时，如果一个进入的邮件匹配一个组合的发件人和收件人而不是发件服务器，但是如果SPF处理决定发件服务器是对组合中列出的发件服务器一个有效的替代，那么这个邮件将被作为一个匹配那个组合的后来的发送尝试来处理，而不是一个全新的需要新的灰名单记录的连接。

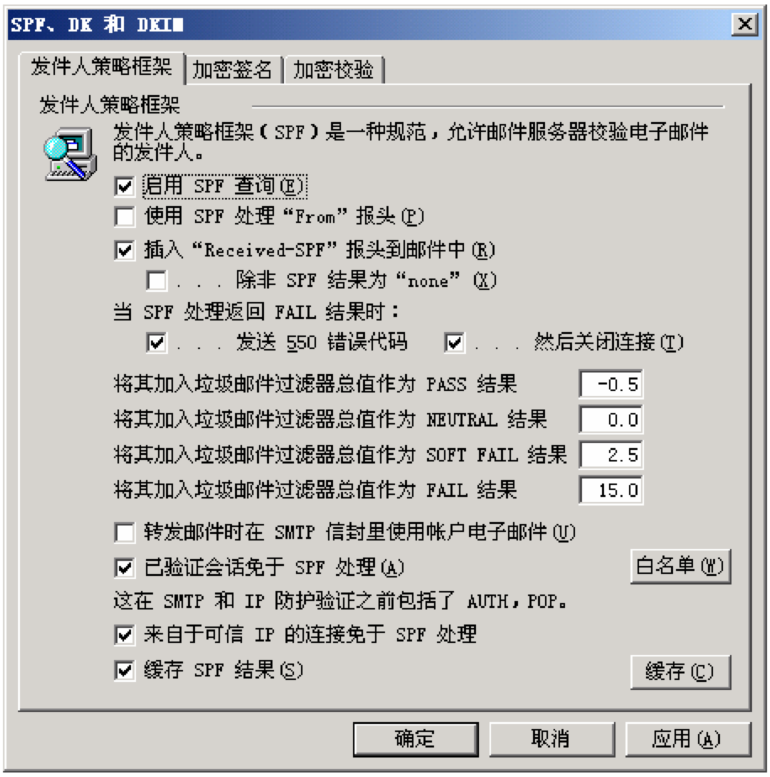
<u>不要对发件人列于本地地址簿的邮件进行灰名单验证</u>
点击这个选项，如果你想让发件人列于收件人地址簿的那些邮件被免除灰名单验证。

<u>不要对发往邮件列表的邮件进行灰名单验证</u>
点击这个复选框，如果你想让发往邮件列表的邮件被免除灰名单验证。

<u>不要对通过被验证的进程发送的邮件进行灰名单验证</u>
使用这个选项，如果你想让所有通过验证进程邮件被免除灰名单验证。

<u>不要对来自被信任的IP地址的邮件进行灰名单验证</u>
使用这个选项，如果你想让所有来自被信任的IP地址的邮件被免于灰名单验证。

发件人策略框架



所有的域都发布MX记录来识别那些可能为其接收邮件的计算机，但这不会识别被允许向其发送邮件的位置。SPF是一种方法，通过它域就能发布“逆向MX”记录来识别那些被授权发送邮件的位置。使用这个标签上的选项来配置你服务器的SPF设置。

更多关于SPF的信息，请访问http://spf.pobox.com。

发件人策略框架

激活SPF查询

点击这个复选框来激活SPF查询—MDaemon将对所有进入的并非来自白名单列表IP地址或被免除，例如经验证的连接或被信任的IP地址（当这些免除都已经被激活）的邮件执行SPF数据查询。

用SPF处理“来自”标题

点击这个选项，如果你想对邮件的“来自”邮件头中发现的地址执行一个额外的SPF查找而不是仅检查在SMTP信封中的发件人。如果包含在“来自”邮件头的地址与在SMTP过程中已经检查过的地址相同，那么双倍的检查是不必要的并且将被跳过。

插入‘接收到的SPF’邮件有到邮件中

点击这个选项，如果你想把“接收到的SPF”邮件头插入到每个邮件中。

…除了当SPF结果是“一个也没有”

激活这个选项，如果你不想在SPF查询结果是"一个也没有"时，把"接收到的SPF"标题插入到一个邮件中。

当SPF处理返回了一个失败的结果：

…发送550错误代码
点击这个复选框如果你想在SPF查询结果是"失败"时发送550错误代码。

…然后关闭连接
激活这个选项，如果你想在发送550错误代码后立即关闭连接。

如下选项需要MDaemon PRO

得到通过结果后添加该值到垃圾邮件过滤器分值
当SPF查询结果是"通过"时，指定你想要添加到邮件的垃圾邮件分值的数值。

得到中立结果后添加该值到垃圾邮件过滤器分值
当SPF查询结果是"中立"时，指定你想要添加到邮件的垃圾邮件分值的数值。

得到软失败结果后添加该值到垃圾邮件过滤器分值
当SPF查询结果是"软失败"时，指定你想要添加到邮件的垃圾邮件分值的数值。

得到失败结果后添加该值到垃圾邮件过滤器分值
当SPF查询结果是"失败"时，指定你想要添加到邮件的垃圾邮件分值的数值。

*当转发邮件时在**SMTP**信封中使用该用户帐号地址*
点击这个选项，如果你想让MDaemon使用这个帐号的email地址来自动转发所有的邮件。这能帮助减少转发的相关问题。通常，转发邮件被使用原发件人的email地址发送，而不是实际进行转发邮件的账号地址。

*经过验证的会话可以免除**SPF**处理*
点击这个复选框，如果你想让经过验证的连接免除SPF查询。经过验证的进程包括那些经过AUTH，SMTP之前POP或IP屏蔽验证的。

白名单
点击这个按钮来打开SPF白名单，从中你可以指定哪些IP地址可以被免除SPF查找。

*来自被信任的**IP**地址的连接可以免除**SPF**处理*
激活这个选项，如果你想让来自被信任的IP地址的连接被免除SPF处理。

*将**SPF**结果加入缓存*
点击这个选项，如果你想临时将SPF查询结果加入缓存。

缓存
这个按钮打开了SPF缓存。

域名密钥和DomainKeys邮件识别技术

域名密钥 DomainKeys（DK）和域名密钥标识邮件技术（DKIM）是使用密码的email验证系统，它能用于防止网络诈骗。而且，因为大多数的垃圾邮件都包含欺骗性的地址，DK/DKIM能帮助从很大程度上减少垃圾邮件，尽管它们不是专门设计用于反垃圾邮件的工具。DK/DKIM还能用于确保收到的邮件的完整性，或确保邮件在发件人服务器被发出直到到达接收者服务器的过程中未曾受到撰改。换句话说，有了DK/DKIM密码验证系统，收件人服务器就能确信到达的邮件是来自发件人的并且没有人用任何方式改变过邮件信息。为了确保邮件的有效性和完整性，DK/DKIM使用一个公共和秘密的keypairs系统。一个加密的公共秘匙被发布到发送服务器的DNS记录，然后每个发出的邮件都被服务器用相应的秘匙作了签名。. 对于收到的邮件，当收件服务器发现一个邮件被作了签名，它将从发件服务器的DNS记录中找回公共秘匙，然后将其与邮件中的签名比对来确定邮件的合法性。如果收到的邮件不能通过验证，那么收件服务器就知道其包含了伪造的地址或曾被篡改。失败的邮件可以被拒收，或者被接收但是会调整其垃圾邮件的打分。

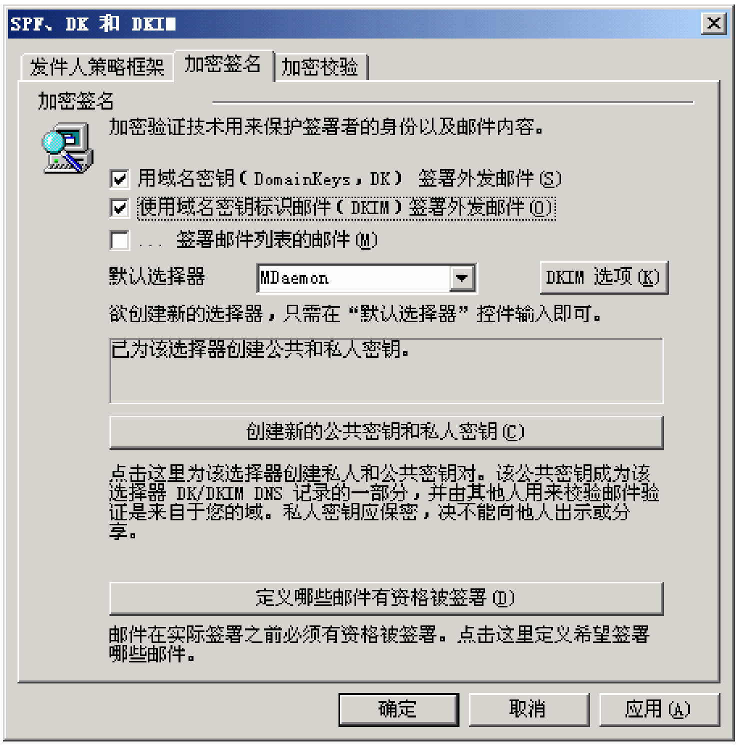
要配置MDaemon来验证进入的被作了加密标记的邮件，使用位于Security>SPF/DomainKeys & DKIM….加密验证标签上提供的选项。要配置MDaemon来签名发出的邮件，使用相同对话框的加密标记标签上的选项。

MDaemon的主界面包含一个DomainKeys标签(位于邮件标签下)，可以被用于实时监控DK/DKIM活动，你也可以使用位于Setup>Logging…>Options的选项把DK/DKIM活动记入日志。

更多关于DomainKeys技术的信息，请访问：
http://antispam.yahoo.com/domainkeys.

更多关于DomainKeys邮件识别技术的信息，请访问：
http://www.altn.com/press/press_release.asp?ReleaseID=137.

加密签名



使用包含在加密签名标签上的选项来控制一些发出的邮件是否将被作上加密签名，使用什么方法来签名它们(DK和/或DKIM)，和指定哪个邮件必须被签名。你也可以使用这个标签来指定选择器和生成适合DK和DKIM规范的相应的公共和秘匙。默认的选择器(“MDaemon”) 和一个默认的公共和秘匙将在启动时自动为你创建。所有的key都是独一无二的—从一个站点到另一个站点，它们决不会相同，不论所指定的选择器是哪个。默认情况下，生成的key都具有安全的1024位。

DomainKeys 签名

用DomainKeys (DK)签署发出的邮件

点击这个选项，如果你想让MDaemon使用DomainKeys为一些发出的邮件作出加密签名。为了让一个邮件被签名，它必须符合“哪些邮件符合签名条件”按钮中指定的标准，并经过验证的进程发送并被MDaemon接收。你还可以使用一个内容过滤器行为“*用DomainKeys选择器进行标记…*” 来签名邮件。

用DomainKeys邮件识别技术(DKIM)签名发出的邮件

点击这个选项，如果你想让MDaemon使用DomainKeys邮件识别技术来对一些发出的邮件作出加密签名。为了让一个邮件被签名，它必须符合“哪些邮件符合标记条件”按钮中指定的标准，并通过验证的进程发送并被MDaemon接收。你还可以使用一个内容过滤器行为“*用DomainKeys选择器进行标记…*” 来签名邮件。

…签名邮件列表邮件

点击这个复选框如果你想对所有发出的邮件列表邮件作出加密签名。因为

MDaemon将签名发送到所有你的列表的所有邮件，你不必使用"定义哪些邮件符合标记要求"选项来授权它们进行加密签名。

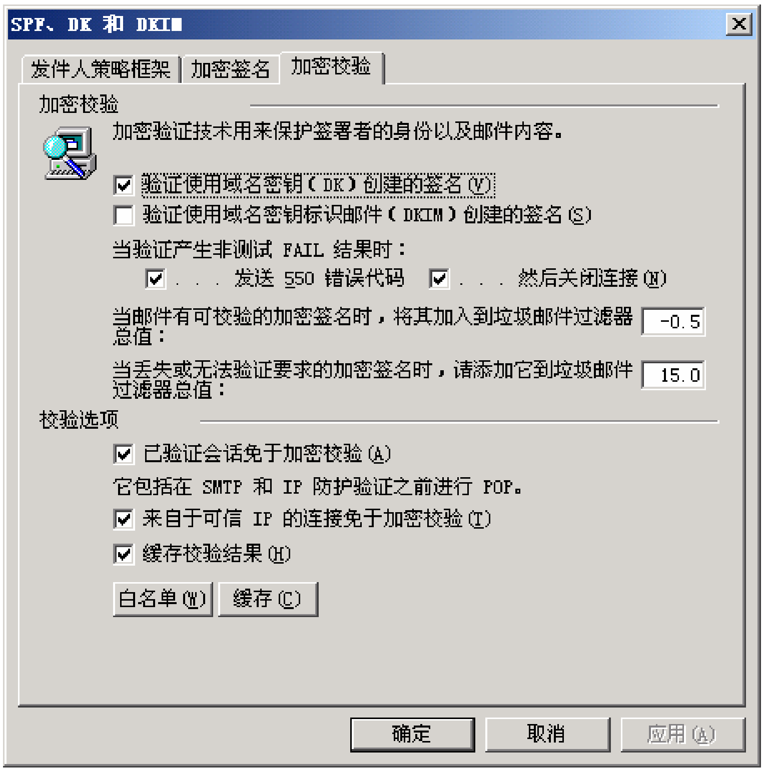
注意
签名列表邮件需要在"分解"列表后对每个列表邮件进行内容过滤处理。在处理大量和高度活跃的邮件列表时，这可能会影响服务器的性能。

默认选择器
从下拉列表中，选择选择器，这个选择器相应的公共/私密key对正是你想让MDaemon用于签名邮件的。如果你想用一个不同的选择器来创建一个新的key对，那么在此输入你想要的选择器名称并点击下面的"创建新的公共和私密*key*"。如果你想使用一个交替的选择器来签名一些邮件，请使用"*用DomainKeys选择器签名…*"行为来创建一个内容过滤规则。

*创建新的公共和私密**key***
点击这个按钮来生成一对公共/私密key用于上述指定的选择器。将为选择器生成一对公共/私密key，还会生成一个dns_readme.txt文件并自动打开。这个文件包含了样本DK/DKIM数据，你需要这些数据来为指定的选择器发布你的DK/DKIM策略和公共key到你域的DNS记录列表。文件列表样本为测试和非测试状态，以及是否你要签名所有邮件或仅仅签名一些来自你的域的邮件。如果你当前正在测试DK/DKIM或这个选择器，那么你需要使用包含在测试条目的信息用于策略或者选择器，取决于你正在测试的内容。否则你就需要使用非测试条目。所有的key都以PEM的格式存储，而且所有的选择器和key都存储在\MDaemon\Pem文件夹下，并以如下方式存储：
`\MDaemon\Pem\<Selector>\rsa.public` - public key for this selector
`\MDaemon\Pem\<Selector>\rsa.private` - private key for this selector

定义哪些邮件符合签名条件
当你已经激活一个或两个上述签名发出邮件的选项，点击这个按钮来编辑DKSign.dat文件，这个文件包含了域的列表和MDaemon将要用于决定是否一个邮件应该被签名的地址。对每个列出的地址，你还必须指定是否这个邮件应该被发往或来自该地址，为了让其符合被签名的条件。此外，你还能为每个条目任意指定一个选择器，这个选择器将在签名一个匹配那个条目的邮件时被使用。最后，你能指定一个任意的签名域在签名标题中的"d="标签中使用。这会非常有用，例如，当你有多个子域签名邮件。在这样的情况下，你可以使用"d="标签来告诉收件服务器在单个域的DNS记录中寻找DK/DKIM key，这样使你能在一个记录中管理所有的key，而不是不得不为每个子域管理单独的记录。在域和地址中允许使用通配符。

加密校验



使用这个标签来配置MDaemon用于在到达的远程邮件寻找DomainKeys (DK)和/或DomainKeys邮件识别技术(DKIM)签名，以及在发现时尝试检验它们。当一个到达的邮件已经被加密签名，MDaemon将从签名服务器的DNS记录中重新找回公共key，然后使用那个key来测试邮件的DK/DKIM签名来决定其有效性。如果签名验证过程返回了一个“失败”的结果，那么MDaemon将重新找回签名域的策略。如果这个策略没有显示DK/DKIM已经过测试，那么这个邮件就会被直接拒绝或向上调整其垃圾邮件分值后被接收。如果一个邮件没有被标记签名，那么MDaemon将在“来自”标题中重新找回域的策略来决定是否那个域的邮件应该被签名以及是否这是测试模式。如果域不仅仅测试DK或DKIM，而且它显示所有的邮件都应该被签名，那么邮件将会收到一个“失败”结果并接受相应处理。当一个邮件没有被签名，而且这个域的DNS记录并不包含一个DK/DKIM策略，那么这个邮件将被正常处理，就好像加密验证没有被使用一样。收到“通过”结果的邮件将继续接受正常处理，并相应调整它们的垃圾邮件分值。

DomainKeys验证

检验使用DomainKeys (DK)创建的签名

点击这个选项来激活DomainKeys验证来自远程的邮件。

检验使用DomainKeys邮件识别技术(DKIM)创建的签名

点击这个选项来激活DomainKeys邮件识别技术验证来自远程的邮件。

当验证产生一个非测试的失败结果:

...发送550错误代码
当这个复选框被激活并且验证过程返回了一个“失败”结果，MDaemon将返回550代码并在SMTP进程中拒绝邮件，除非签名域的DomainKeys策略显示其仅仅测试DK/DKIM。如果域的策略显示其正在测试，那么邮件将被正常处理。

...然后关闭连接
点击这个选项，如果你想在DK/DKIM验证邮件收到了一个“失败”结果并且该邮件根据先前的选项被拒绝后关闭一个发件服务器的连接。如果这个选项被禁用，那么邮件根据先前的选项仍然将被拒绝，但是连接将继续。

当一个邮件有一个可验证的加密签名时添加这个到垃圾邮件过滤器分值
这里指定的值将被添加到任何收到“通过”结果被DomainKeys或DomainKeys邮件识别技术标记的邮件的垃圾邮件分值中。

注意

通常这里指定的值应该是一个负值，这样包含有效加密签名的垃圾邮件分值就会减少。然而，当为这个值赋值时你应该小心对待，因为一些垃圾邮件发送者已经开始对其邮件进行签名，一个邮件被标记并不能保证它不是一个垃圾邮件。MDaemon对于这个选项的默认值是-0.5。

当一个必需的加密签名丢失或未能被检验时添加这个到垃圾邮件过滤器分值
当上述的“...发送550错误代码”选项被禁用并且发件域的策略没有显示DK/DKIM正在被测试时，这里指定的数值将被添加到任何DomainKeys或DomainKeys邮件识别技术标记的收到“失败”结果邮件的垃圾邮件分值中。当站点的策略显示测试，一个失败的加密验证将不会引起垃圾邮件分值以任何方式被修改。

验证选项

经过验证的连接免于加密验证
点击这个选项，如果你想让某个通过AUTH，在SMTP前的POP，或IP屏蔽验证的的邮件连接免于加密验证。

*来自被信任的**IP**地址的连接免于加密验证*
使用这个选项，如果你想让来自被信任的IP地址的连接免于加密验证。

缓存验证结果
点击这个选项，如果你想缓存在DNS查找中找到的DK/DKIM信息。通过临时缓存包含在一个域的DNS记录中的信息，你能增加处理从相同域处到达的DK/DKIM签名邮件的效率。

白名单
点击这个按钮来打开排除列表。源自这个列表中指定的任何IP地址的邮件都不会

接受加密验证。

缓存

这个按钮打开了DomainKeys缓存。当使用上述的*缓存DomainKeys结果选项，这个文件将列出任何当前被缓存的信息。*.

验证结果邮件头

无论何时，一个邮件使用SMTP AUTH，SPF，DomainKeys，或DomainKeys邮件识别技术进行验证，MDaemon将插入验证结果标题到邮件中，列出验证处理的结果。如果MDaemon被设置成即使当邮件没有通过验证也接受邮件，那么验证结果标题将会包含一个代码来描述失败的原因。

第十章

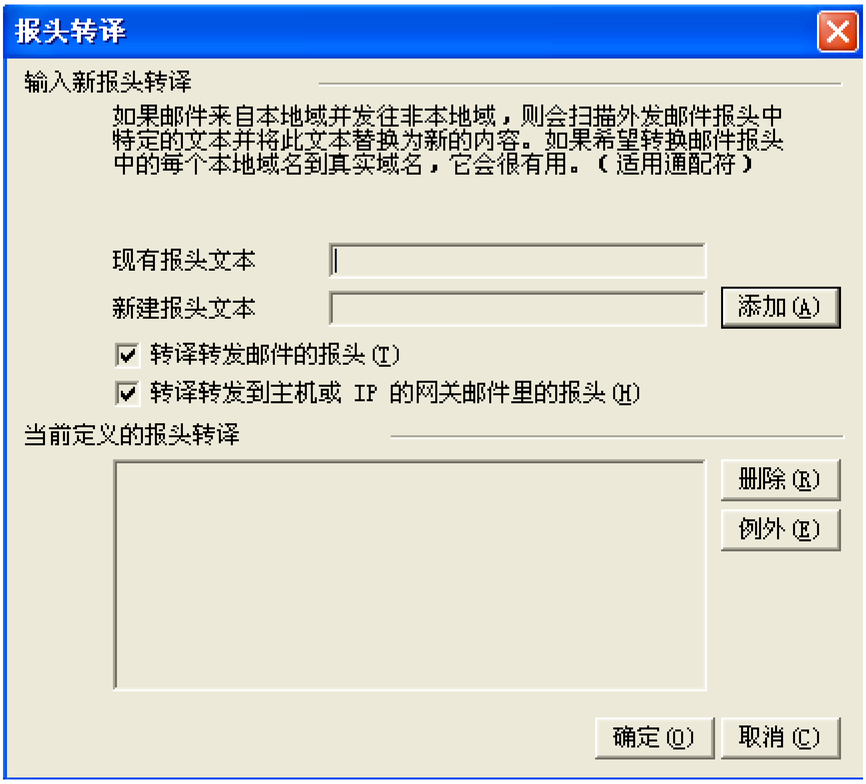
MDaemon ® 中文版

报头转译

报头转译

如果你有邮件要在因特网上收发，而邮件必须要包含你的域名，可以使用邮件头转换功能替换邮件头中文本的任何部分。你可以指定邮件中的想要被替换的文本和相应的替换值。Mdaemon 将查找邮件中所有的邮件头，然后替换。还可以通过打开排除按钮指定哪些邮件头 Mdaemon 是不应该修改的（列如“标题”或“收件人字段”）。

这个功能对于一些本地域名和伪造或不合法的或和外发邮件显示的域名不一样的Mdaemon设置是非常必要的。在这种情况下，邮件转换可以转换“@localdomain.com”到“@RemoteDomain.com”。



输入新报头转译

现有的报头文本

输入当在任何外发的邮件中存在并希望替换的文本。

新建报头文本
这个文本将会被用来替换*现有的邮件头文本*区域指定的那个。

添加
点击此按钮添加以上文本参数到当前邮件头转换列表。

转译转发邮件的报头
点击此复选框的邮件头转换也应用到从一个本地域自动转发到一个非本地域的邮件中。

转译转发到主机或 IP 的网关邮件里的报头
如果你希望邮件头在转发的域网关邮件中被转换，点击此复选框。更多信息，参看网关编辑器上的邮件转发标签。

当前定义的报头转译
此列表包括一些文件信息，MDaemon 将会对外发邮件邮件头检查以及当发现匹配时，将用该文本替换。

移除
在当前邮件头转换列表中选择一个条目，然后点击此按钮从列表中移除它。

例外
点击此按钮打开邮件头转换例外对话框。这个对话框用来指定任何你希望从邮件头转换过程中忽略的邮件头。

报头转译例外

不要转译在这些报头中的值
报头值
输入你希望从邮件头转换过程中忽略的任何邮件头。

添加
点击此按钮来添加一个新邮件头到列表。

排除这些报头
当替换邮件头文本时，MDaemon 将不会检查这些邮件头。

移除
在列表中选择一个邮件头，然后点击此按钮移除它。

第十一章

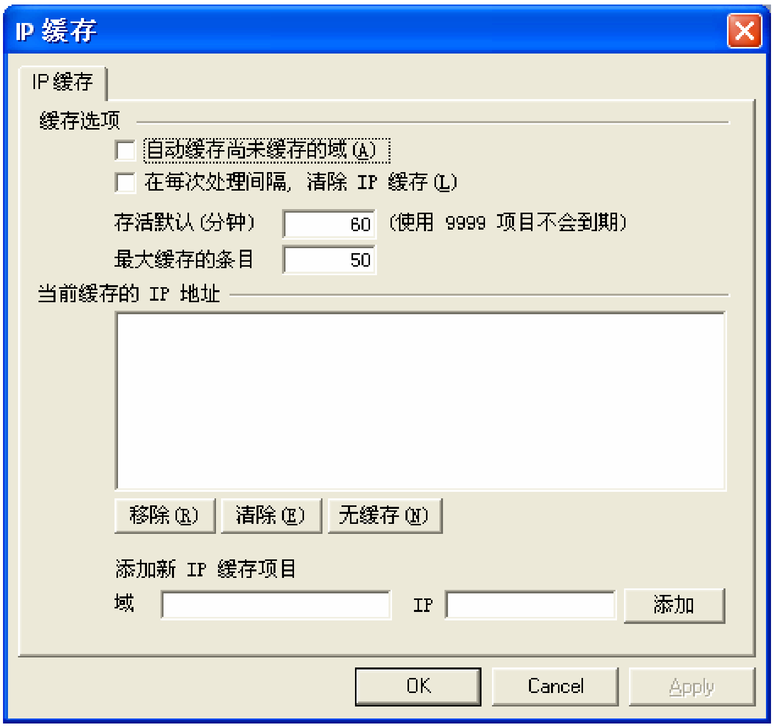
MDaemon ® 中文版

IP缓存和DNS查询

使用IP缓存和执行DNS查询

为了加速邮件投递和减短邮件处理时间，MDaemon 缓存所有来自联系人的主机 IP。这些 IP 被存储下来，并且每次 MDaemon 在域名上要求 DNS 解析时，都将检查缓存。如果需要解析的域名在 IP 缓存中找到，则跳过 DNS 查询，这可以节省大量的处理时间。在窗口中的此设置允许你在将处理的缓存的参数。你也可以手动添加并移除条目，以及设置缓存的最大量。IP 缓存可以在设置 – IP 缓存…菜单选项中打开。

IP缓存



缓存选项

在每次处理间隔点，清除 IP 缓存

如果选择，缓存的条目内容将在每次邮件会话开始时被清掉。这允许在每次处理间隔刷新缓存。

自动缓存尚未缓存的域

此开关控制 MDaemon 的内在的自动缓存引擎。如果你希望 MDaemon 自动缓存

域，则启用此选项。如果你希望自己创建 IP 缓存，则清空此检查框。

存活默认（分钟）
这是 IP 缓存中存活的时间的默认值。一旦条目在缓存中存在了这么长时间，MDaemon 将会移除它。如果你指定默认时间为 9999，在这种情况下，条目永远不会过期。
最大缓存条目
这个值决定了缓存可能为多大。一旦达到这个设置，下一个缓存条目将会把第一个条目顶出。

当前缓存的 **IP** 地址
移除
在当前缓存 IP 窗口中选择条目，之后点击此按钮移除它。

无缓存
点击此按钮提出你不希望 MDaemon 添加到 IP 缓存的域名称和/或 IP 地址列表。

清除
此按钮将会清空缓存。

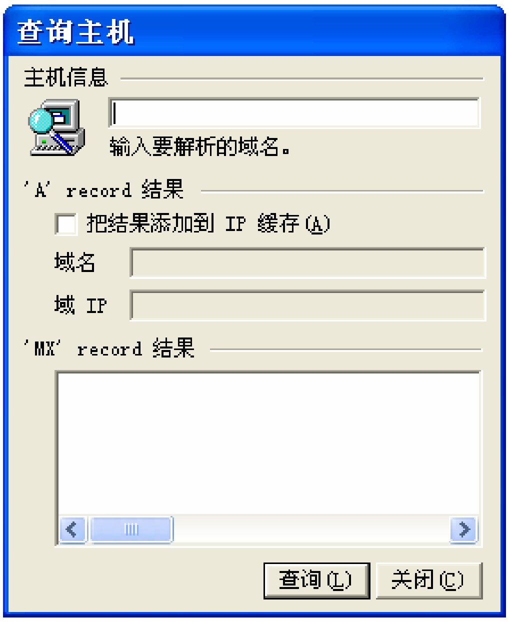
添加新 **IP** 缓存条目
域
输入你希望添加到 IP 缓存的域名称

IP
输入你希望添加到 IP 缓存的 IP 地址。

添加
一旦你已经输入了一个域名称和 IP 地址，点击此按钮手动添加它们到缓存。

DNS查询

DNS 查询功能（设置 – 执行 DNS 查询…）在用于与 IP 缓存协同工作时，是非常有效的。DNS 查询可以使你快速和简便的对任何合法的 Internet 域名执行 DNS 查询成为可能。一个成功的解析域名查询将会显示域的 A-Record 和任何可能列出的 MX-Record。也有用来能够自动添加成功查询结果到 IP 缓存的控制。



主机信息
输入你希望重新得到 DNS 信息的域名

"A" record 结果
把结果添加到 IP 缓存
如果你希望 DNS 查询结果添加到 IP 缓存，点击此复选框。

域名
这是解析的域名的名称。

域 IP
这是解析的域 IP 地址。

"MX" Record 结果
此窗口显示任何被解析的域所列出 MX 记录。

查询
点击此按钮为在主机信息部分你已经列出的域名称执行 DNS 查询。

第十二章

MDaemon ® 中文版

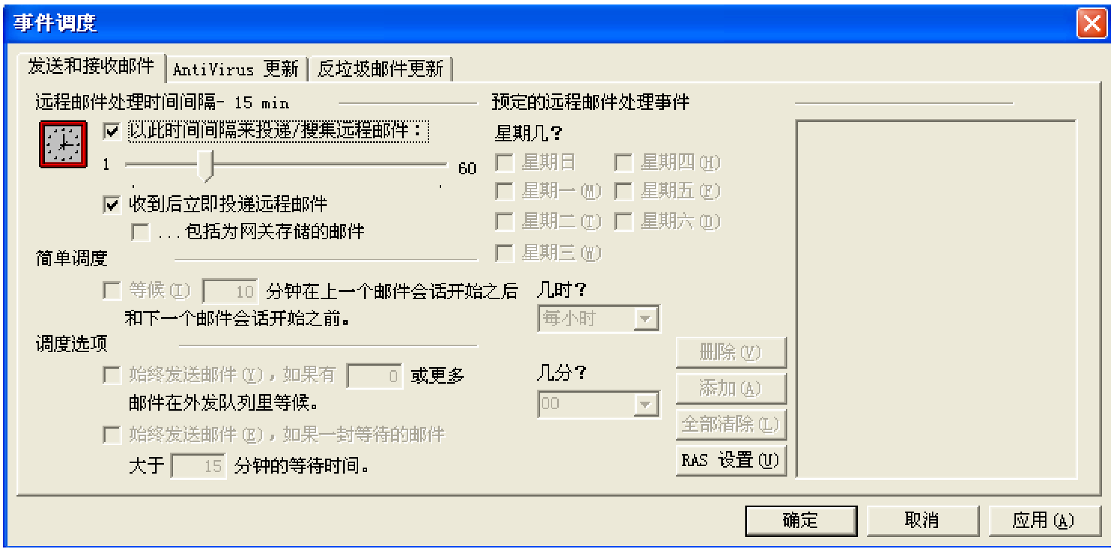
事件调度和拨号

使用日程安排和**RAS**拨号引擎

点击**设置 – 事件调度...**菜单选项（或者按下 F6）来打开 MDaemon 事件日程安排程序。此对话框使你安排 MDaemon 的远程邮件处理进程尽可能简单成为可能。你可以为邮件投递和收集安排精确的次数，或者在正常的间隔上，使用一个计数器来处理邮件。你也可以设置在未安排次数时，触发邮件处理的条件，比如当一定数量的邮件等待发送时，或者一个邮件已经等待了指定的时间。如果你安装了支持 MDaemon 的 Alt-N 的 AntiVirus，在此对话框上将会有一个称作 AntiVirus 更新的附加标签。这个标签用来安排对 AntiVirus 病毒签名更新检查的时间。

事件调度

发送/接收邮件



远程邮件处理间隔

使用此间隔，递送/收集远程邮件

点击复选框并且滑动这个栏向左或者向右，可以为邮件处理会话指定时间间隔。它可以配置成从 1 到 60 分钟的范围。在此时间后，MDaemon 将会在再次开始计数处理远程邮件。当清空此复选框，此对话框上的其它时间安排选项将会决定远程邮件处理间隔。

收取后即时递送远程邮件
当选择此选项时，MDaemon 当收到邮件时，将立即处理并投递远程邮件，而不是等待下一个处理间隔。

***...**包含网关存储的邮件*
如果你希望域网关的邮件能够立即发送，点击此复选框。但是，这只能把网关编辑器的网关标签上启用的"*在每次安排远程邮件处理间隔投递邮件*"选项应用到网关。

简易调度

在 MDaemon 中有很多触发远程邮件会话的方式。当你希望在正常时间间隔内处理远程邮件而无论是否条件触发会话，*简易计划*功能是非常便利的。与设置指定的时间或者使用滑动栏指定的严格的固定间隔不同，此选项的时间间隔无论何时处理邮件都将被重置，而不管什么导致了邮件会话初始化。

注意：
为了简单时序安排能够在指定的日子生效，至少一个定时的条目必须存在于那天的*日程安排列表*中。例如，假设你希望在拨号会话之间安排 45 分钟，而且只在周一至周五生效。你会需要启用简单的时序安排选项，并且输入 45 分钟到此控制中，然后对每一天输入至少一个安排的时间（周一，周二，周三，周四，周五）。由于在周六或者周日没有安排的时间，这两个日子将会被免除，并且不会触发远程邮件会话。当你设置你的触发日时，你指定的小时和分钟设置没有任何影响；简单的时序安排只检查在那天是否有一个条目存在。

调度选项
总是发送邮件如果有 ***xx*** *或更多邮件在发送队列等待。*
无论什么时候在外送队列中的邮件达到或者超过了你在此指定的数量，MDaemon 都将会触发邮件发送。这些会话将会是任何其它正常的计划的补充。

如果等待邮件超过 ***xx*** *分钟*
当控制启用时，无论在外送队列中一个邮件已经等待了多长时间，MDaemon 将会触发一个邮件会话。这些会话将会是任何其它正常的计划的补充。

计划的远程邮件处理时间
哪一天？
选择你希望计划的日期。

几小时？
选择你希望计划的小时。

几分？
选择你希望计划的分钟。

添加
一旦你已经选择了日期，小时和分钟，点击此按钮添加此时间到此时间安排事件的列表。

移除
点击此按钮将会移除一个你已经从安排列表中选择的条目。

全部清除
此按钮移除所有在安排列表中的条目。

RAS 设置
提供此按钮，你可以快速察看或者编辑你的 RAS 设置。

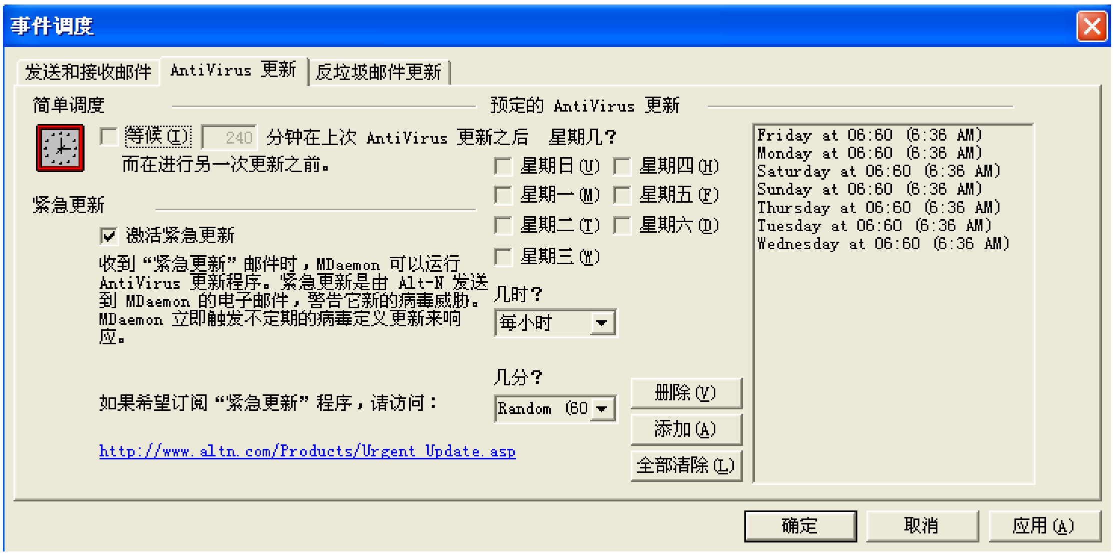
提示：

更多配置将对简单使用滑动栏或者简单时序安排来控制邮件处理间隔是很有益处的。例如，当你可以简单设置滑动栏一分钟间隔将其放入控制，并完成相同的事情时，使用日程安排程序对每一天的每一个分钟进行计划是毫无意义的。另外一方面，如果你希望处理间隔超过一个小时，或者只在某天时，则你可以使用简单时序安排和指定次数的组合。

参看：

配置你的 RAS 设置 – 203 页

AntiVirus更新



简易计划

在进行上次 AntiVirus 更新后，等待 xx 分钟，进行下次更新
点击此复选框，指定你希望 MDaemon AntiVirus 在检查新的病毒定义更新前等待的时间量。注意，这是 MDaemon AntiVirus 在你上次检查更新后进行下次更新等待的实际时间，不管是否通过日程安排程序或手动触发更新。时间安排程序和手

动触发更新比简单时序安排上有优先权，并且如果一个 AntiVirus 更新事件被那些其它方法之一所触发，那么因此它将重置此计数器。例如来说，如果你将此选项设置成每 240 分钟检查更新，并且在 100 分钟之后你手动检查更新，则此计数器将会在 240 重新开始。

紧急更新

激活的紧急更新

点击此复选框激活紧急更新功能。利用开启此功能，无论何时 MDaemon 收到一个“紧急更新”消息，MDaemon AntiVirus 将会立即连接到更新位置并且下载高优先权的更新。接受这些消息，你必须首先订阅在 http://ww.altn.com/Products/Urgent_Update.asp 的“紧急更新”邮件列表。更多信息，参看 Antivirus Updater（241 页）。

预定的 **AntiVirus** 更新

哪一天？

选择你希望计划的日期。

几小时？

选择你希望计划的小时。

几分钟

选择你希望安排的分钟。

添加

一旦你已经选择了日期，小时和分钟，点击此按钮添加此时间到此时间安排事件的列表。

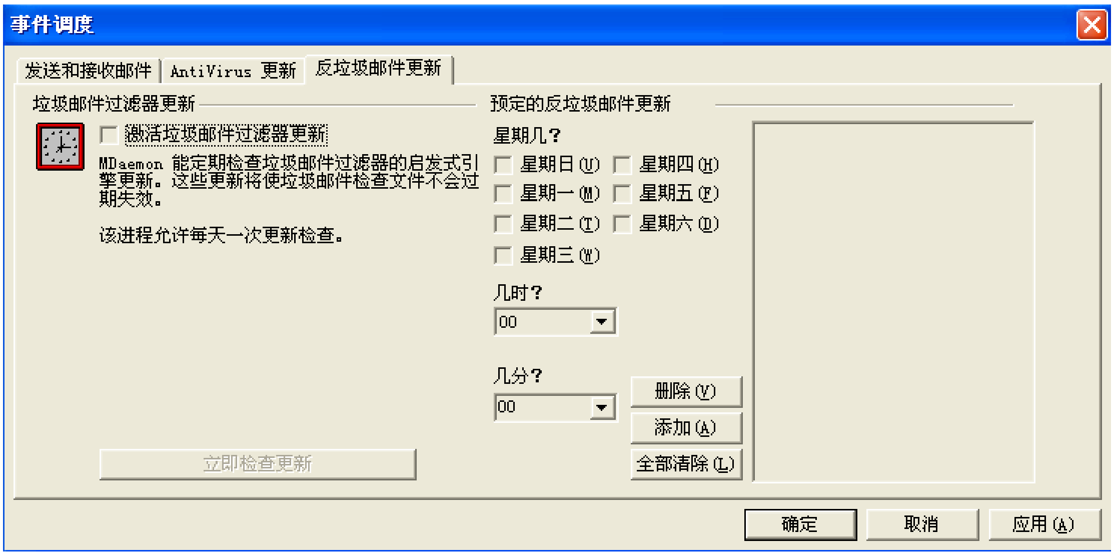
移除

点击此按钮将会移除一个你已经从安排列表中选择的条目。

全部清除

此按钮移除所有在安排列表中的条目。

反垃圾邮件更新



同 AntiVirus 更新标签类似，使用此标签来计划你希望检查新垃圾邮件过滤器规则的频率。由于垃圾邮件规则更新不像病毒定义那么频繁，并且没有那么急切，因此我们建议每周只安排一次检查。如果你希望更多的检查更新，每天一次则是可被安排得最大极限。但是你按你希望的频率可以使用“现在检查更新”按钮。可能很长时间不会有一个更新，但是无论何时有的话，将会发给你指定的内容过滤器管理员一封消息（安全 – 内容过滤器… - 管理/附件）来详细的说明发生了什么。

垃圾邮件过滤器更新

激活垃圾邮件过滤器更新

如果你希望垃圾邮件过滤器规则自动更新，点击此复选框。同 MDaemon AntiVirus 更新功能类似，垃圾邮件过滤器可以在安排的间隔连接到 Alt-N Technologies 来检查新的规则，然后在找到时，自动下载并安装它们。

马上检查更新

点击此按钮立即检查一个垃圾邮件过滤器规则更新。

预定的反垃圾邮件更新

哪一天？

选择你希望计划的日期。

几小时？

选择你希望计划的小时。

几分？

选择你希望计划的分钟。

添加

一旦你已经选择了日期，小时和分钟，点击此按钮添加此时间到此时间安排事件的列表。

移除

点击此按钮将会移除一个你已经从安排列表中选择的条目。

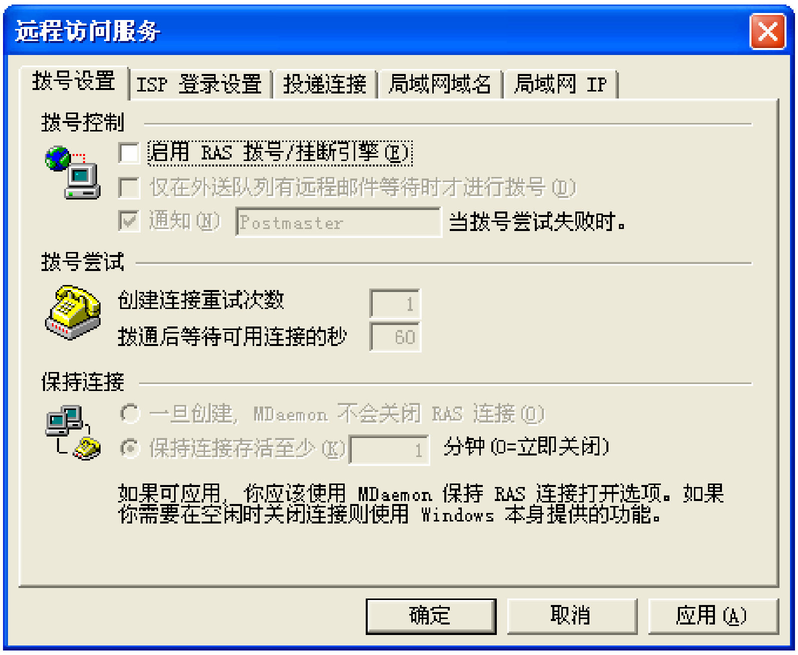
全部清除

此按钮移除所有在安排列表中的条目。

RAS拨号设置

点击设置 – RAS 拨号/挂断…菜单选项（或者按 F7）来配置你的 RAS 拨号设置。此对话框只有在你将远程访问服务安装到你的系统时才可用。当你需要拨号到你 ISP 时，MDaemon 只在远程邮件处理事件前可以使用它。

拨号设置



拨号控制

*启用 **RAS** 拨号/挂断引擎*

选择此选项将会导致 MDaemon 在发送和/或接受远程邮件时，使用在此指定的设置来连接远程主机。

仅在外送队列有远程邮件等待时才进行拨号

当启用此开关，MDaemon 将不会对 ISP 拨号，除非在远程队列中有远程邮件等待。在某些环境中，这是非常有益的，但是要考虑到 MDaemon 是否没有拨号，那么则它不能做任何邮件收集工作（除非它通过本地 LAN 发送）。

通知[地址]当拨号尝试失败时

当选择了此选项，当拨号失败时，MDaemon 将会发送消息到指定的地址

拨号尝试

创建连接重试次数

在放弃前，MDaemon 将会尝试连接远程主机这么多次。

拨通后等待可用连接的秒

这个值决定了 MDaemon 将等待远程计算机多长时间来应答并完成 RAS 连接。

保持连接

一旦创建，MDaemon 不会关闭 RAS 连接

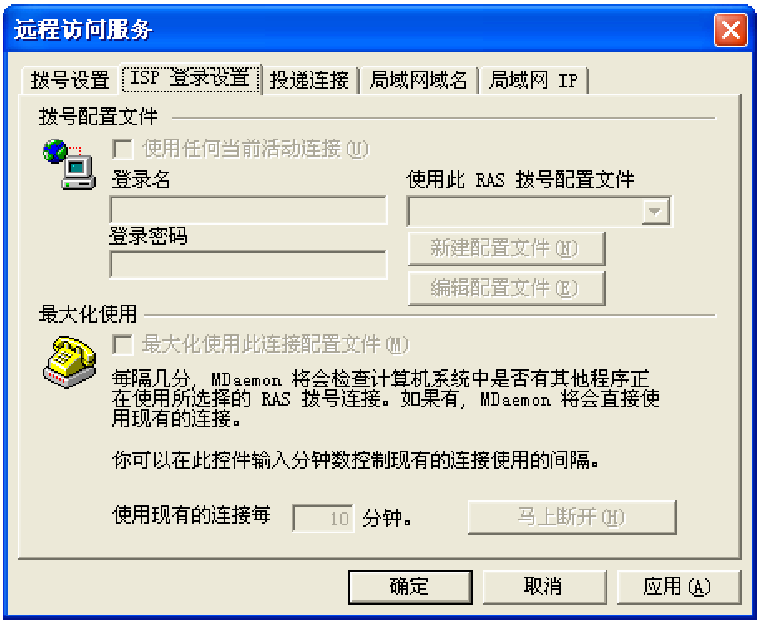
默认值，在所有邮件处理完成后，MDaemon 将会立即关闭一个已经创建的连接，并且不会再使用此连接。设置此选项将会导致连接保持，即使所有的处理已经完成。

注意：
MDaemon 不会关闭一个没有创建的连接。

保持连接存活至少 xx 分钟

如果启用，此选项将会使一个 MDaemon 创建的 RAS 连接保持开放至少指定的分钟，或者知道所有的邮件处理已经完成，这取决于哪个值更合适。

ISP登录设置



拨号配置文件

使用任何当前活动连接

如果你希望 MDaemon 在其检测到有活动连接时，能够利用其它的连接配置文件，那么请点击此检查框。无论什么时候进行拨号，MDaemon 将首先查看是否有它可以使用的连接，而不是先拨号。

登录名

在此指定的值将会在认证过程期间被传送到远程主机。

登录密码

在此指定的值将会在认证过程期间被传送到远程主机。

*使用此 **RAS** 拨号配置文件*

此下拉列表框允许你选择一个已经预先定义过的连接配置文件，此文件是通过窗口拨号网络或者远程访问服务设置的。

新建配置文件

点击此按钮创建一个新的拨号网络或者远程访问服务配置文件。

编辑配置文件

点击此按钮编辑当前选择的拨号网络或者远程访问服务配置文件。

最大化使用

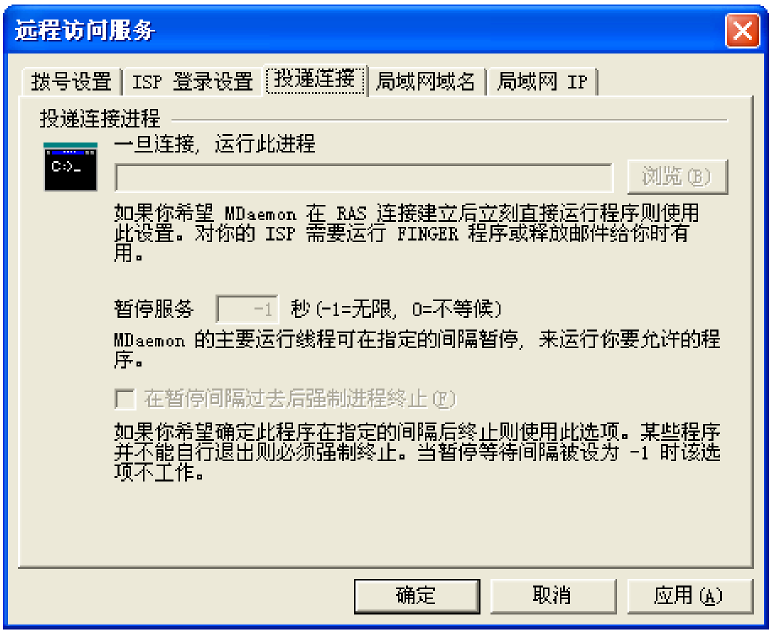
最大化使用此连接配置文件

此设置使 MDaemon 监视你的连接，如果如果它检测到另一个程序创建了一个连接，那么它将立即处理远程邮件，而忽略已安排的时间。如果连接保持开放，它将在基于*使用现有的连接每 xx 分钟*设置上的正常的时间间隔来处理远程邮件。

马上断开

此按钮将会关闭到 ISP 的连接。此按钮只有在 MDaemon 已经初始 RAS 连接的情况下才活动。

投递连接



投递连接进程

一旦连接，运行此程序

如果在此指定程序，MDaemon 将会产生一个线程，并执行此程序。这对那些需要 Finger 或者一些其它的程序访问 ISP 的邮箱是非常有用的。

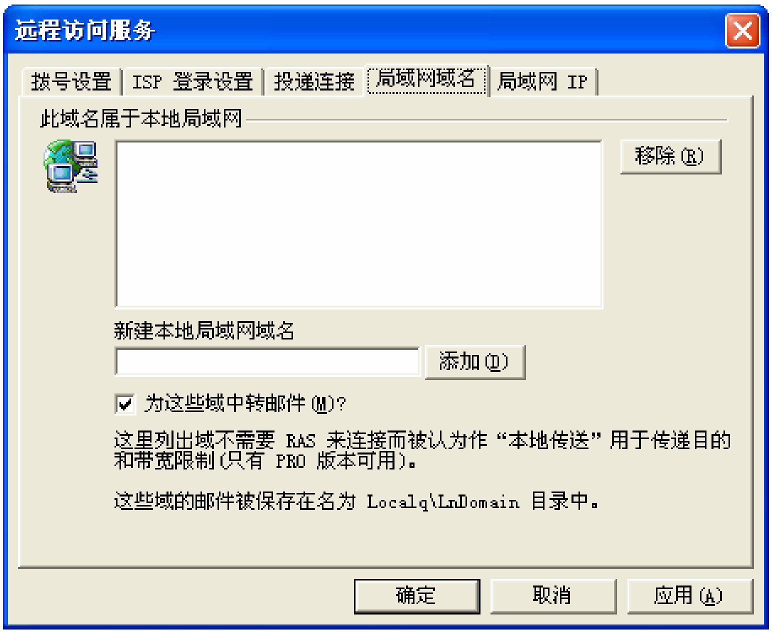
暂停服务 xx 秒（-1=无限，0=不等候）

如果*一旦连接，运行此程序*选项包含合法条目，则在服务器等待执行进程返回时，服务器将会暂停它的处理在此指定的时间。输入“-1”将会使服务器无限的等待直到进程返回。

在暂停间隔过去后强制进程终止

有时，你需要运行一旦运行可能不能退出的程序；一些程序需要用户来干涉以便能关闭他们。当软件必须不被注意的运行时，这是不可接受的。如果选择了此开关，一旦经过了暂停服务 XX 秒选项中指定的时间，则 MDaemon 将会强制处理进程终止。当服务器配置成用来无限的等到进程返回时，此功能不会工作。

局域网域名



此域名属于本地局域网
这所列的域被 MDaemon 当作是你的本地 LAN 的一部分。因此，为了发送向它们其中之一发送邮件，不需要拨号。

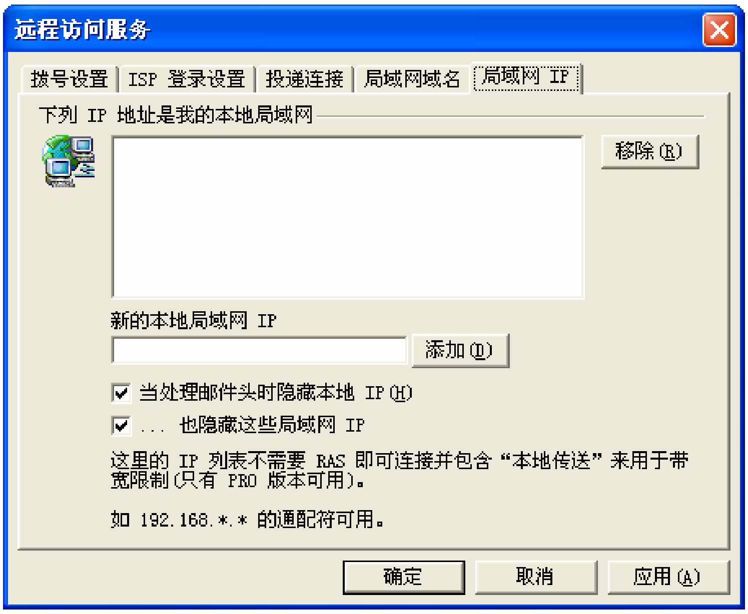
新建本地局域网域名
输入一个域名添加到本地 LAN 列表，然后点击添加*按钮*来添加它。

为这些域中转邮件
如果选择了此选项，MDaemon 将会为这些域中转邮件。这将提供了对发到或者来自到这些域通信量的控制方法。

添加
点击添加按钮来添加一个条目到 LAN 域。

移除
点击此按钮从 LAN 域的列表中移除一个选择的条目。

局域网IP



注意：此对话框与在 RAS 拨号和安全设置上同样名字的对话框时一样的。在这些对话框的任何一个上，更改此设置将会在所有设置上都显示出来。

下列 IP 地址是我的本地局域网

此标签用来列出在你的局域网（本地区域网络）IP 地址。因此这些 IP 地址不需要 RAS 来连接，并且出于减少占用带宽的目的，它们被作为本地通信量。而且由于他们是本地地址，所以在各种其它的安全和垃圾邮件阻止限制中，可以被免除。

移除

从列表中选择一个 IP 地址，然后点击此按钮移除它。你也可以双击一个条目来移除它。

新的本地局域网 IP

输入一个 IP 地址添加到本地 IP 列表，然后点击添加。类似于 127.0.*.*的通配符是允许的。

添加

在输入一个 IP 地址到新的本地局域网 IP 控制，点击此按钮添加到列表。

第十三章

MDaemon® 中文版

DomainPOP邮件收集

使用MDaemon的DomainPOP邮件收集功能

使用 DomainPOP 邮件收集（**设置 – DomainPOP…，或者 F8**）来配置 MDaemon 从远程 POP 邮箱下载邮件再分发到你的用户。此功能可以通过 POP 协议使用指定的登陆信息来下载 ISP 的邮箱的邮件。一旦下载完成，根据设置来处理邮件然后分发到用户的邮箱或者 Mdaemon 的远程队列来发送。

值得注意的是，在 POP 邮箱里面存储的和通过 POP 协议收下的邮件将缺少重要的路由信息（有时被称为邮件信封）。这些信息如果是用 SMTP 协议来处理通常会有的。没有这些信息，Mdaemon 强制检查这些邮件头来决定邮件的来源。邮件头由于缺乏必要的信息通常很难决定邮件的接受着。这种缺乏的信息似乎是正常邮件的必要信息-收件人-但是必须知道，如果使用 POP 协议，邮件是不会被发送到收件人的。使用 SMTP，由于协议本身在传递会话中和服务器使用命令交互，所以邮件内容和收件人是不相关的。

为了让 POP 接收邮件和传递邮件更加可靠和协调，Mdaemon 使用了一套强大的邮件头处理引擎。当 Mdaemon 从远程 POP 下载邮件，立即会处理邮件中相关的邮件头，然后创建相关的收件人。每个邮件头中的邮件地址都会被 Mdaemon 检查并收集。

当进程结束的时候，Mdaemon 收集的收件人表被分为本地和远程。所有被处理和被收集的潜在的收件人地址，在分为本地和远程只前都将经过地址别名转换。

每个本地集合地址的成员都将会收到一封邮件的拷贝。对于远程集合地址，在这个对话框中设置。你可以选择简单的忽略这些地址，转发概要列表到管理员—或 Mdaemon 将传递邮件到远程收件人。只有在很少的情况下，才有需要把邮件传递到远程收件人。

必须要注意防止产生多重邮件或无限制的邮件传递循环。一个常见的问题就是邮件列表的邮件丢失标识自己的 SMTP 信封。典型的，由邮件列表分发的邮件通常在邮件体中不包含任何和收件人相关的地址。邮件列表引擎把邮件列表名字插入到 TO：字段中去。这导致接下来的问题：如果 TO：字段包含邮件列表名称而 Mdaemon 下载完这封邮件，处理 TO：字段（邮件列表名称），然后把邮件分发到相同的邮件列表。这将导致发送该邮件的备份到 Mdaemon 下载该封邮件的 POP 邮箱—从而又导致了整个循环。为了解决这个问题，邮件管理员必须小心使用 Mdaemon 提供的工具来删除邮件列表邮件，或使用别名来把信件投递到相应的邮箱。你也可以利用邮件路由规则或内容过滤器来发邮件投递到正确的收件人。

另外一个问题就是当使用这种邮件收集方法会产生意想不到的邮件副本。如果使用 DomainPOP,对于使用 SMTP 投递到 ISP 的 POP 邮箱的邮件来说很容易就

会产生邮件副本。假设一封邮件发送给你域中的某个人，抄送给该域的另外一个人。在这种情况下，SMTP 将发送该邮件的两份拷贝到 ISP 的邮箱。每份拷贝将会包含相同的收件人—TO：字段和 CC：字段。Mdaemon 会收集这两封相同的邮件而后会处理每个邮件的地址。这将会导致每个收件人都会收到两封相同的邮件。为了避免这种情况，Mdaemon 设置将检查指定一个邮件头来看看是否被复制。Message-ID 就是个好注意。在以上的例子中，两个相同的邮件包含相同的 Message-ID 值。Mdaemon 可以使用这个值标识在下载邮件并且地址信息被处理前删除第二封邮件。

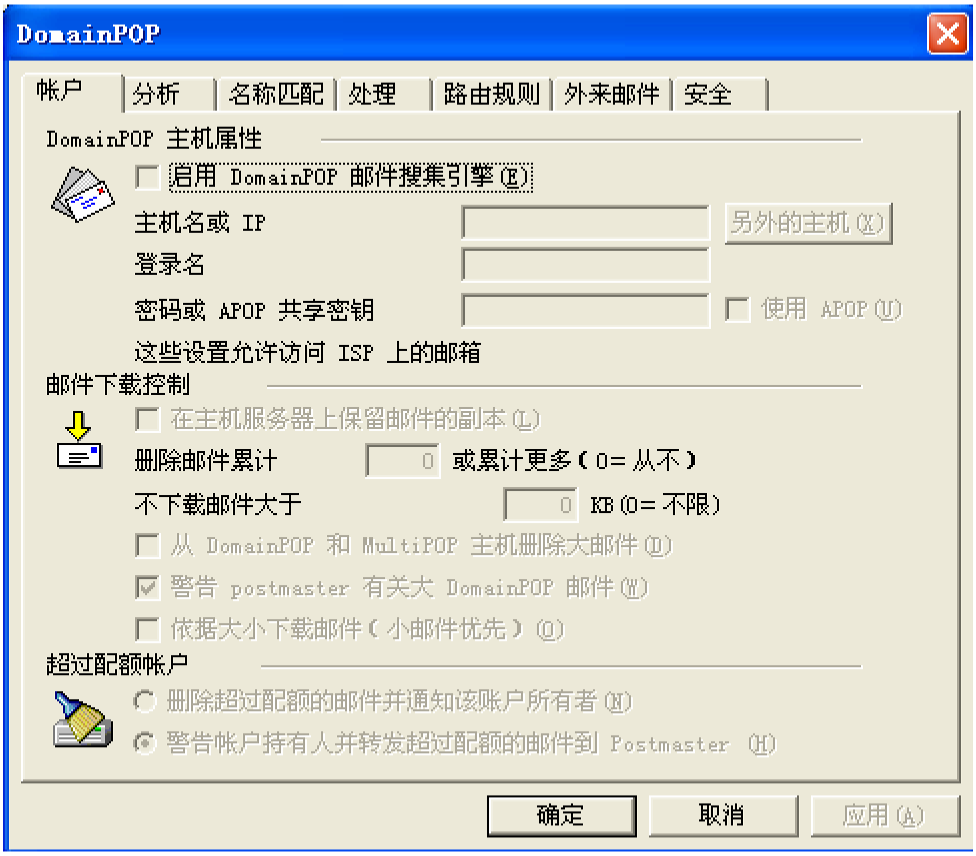
作为一个解决复制邮件和终止邮件传递循环的最终解决办法，Mdaemon使用一种方法来衡量在邮件传递过程中邮件经过多少跳。当SMTP服务器每次处理一封邮件时，都会将邮件加上一个“Received”邮件头。当Mdaemon第一次接收到该邮件时，计算所有这样的邮件头。如果总的数量超过一个指定的值，很有可能该邮件进入一个传递循环了而应该被放到一个坏的队列里去。这个值可以在域配置编辑器指定。

查看：

主域配置—35 页
内容过滤器—240 页
邮件列表—364 页

DomainPOP邮件收集

帐号



DomainPOP 主机属性

启用 DomainPOP 邮件收集引擎

如果选择，MDaemon 将会使用在此屏幕上提供的设置来从 DomainPOP 邮件主机收集邮件然后再分发给本地用户。

主机名或 IP

输入你的 DomainPOP 主机的域名称。另外，如果你希望指定一个端口来收集邮件而不是 MDaemon 当前默认 POP 端口，你可以通过附加一个新的端口值到主机名中，通过冒号分隔。例如，使用“mail.altn.com”作为一个 DomainPOP 主机将会连接到使用默认 POP 端口的主机，而使用“mail.altn.com:523”将会在 523 端口上连接到主机。

登录名

输入 DomainPOP 使用 POP 帐号的登陆名。

密码或者 APOP 共享密码

在此输入 POP 帐号的密码或者 APOP 共享密码。

使用 APOP

如果你希望在收集你的邮件时，使用 APOP 命令和 CRAM-MD5 认证，点击此框。这将使你不必再发送明文密码来认证。

邮件下载控制

在主机服务器保留邮件副本

如果选择，MDaemon 将不会从你的 DomainPOP 邮件主机移除收集的邮件。

一旦超过[xx]封邮件，就进行删除（0=永不）

如果你在你的 ISP 服务器上留下了邮件，则它们在达到此值将会被删除。如果你希望邮件不管数量如何都保留在服务器上，输入“0”。

注意：
一些 ISP 可能限制你允许存储在你的邮箱中的数量。

不要下载大小超过[xx]KB 的邮件（0=无限制）

超过或者等于此大小的邮件将不会从你的 DomainPOP 邮件主机上下载。如果你希望 MDaemon 不考虑大小下载邮件，输入“0”。

从 DomainPOP 和 MultiPOP 主机删除大的邮件

点击此开关，MDaemon 将会删除超过你设置的最大大小的邮件，邮件可以方便的从 DomainPOP 和 MultiPOP 邮件主机中移除，并且将不再下载。

警告管理员“Postmaster”有大的 DomainPOP 邮件

点击此开关，无论何时在 DomainPOP 邮箱中发现一个大的邮件，MDaemon 将会发送一个警告给 postmaster。

根据邮件大小下载（小邮件优先）

如果你希望邮件根据邮件的大小下载顺序，点击此检查框 - 从最小的开始，一直处理到最大的。

注意：
此选项可以更快的找回更小的邮件，但是要求大量的排序和处理。

超过限额的帐号

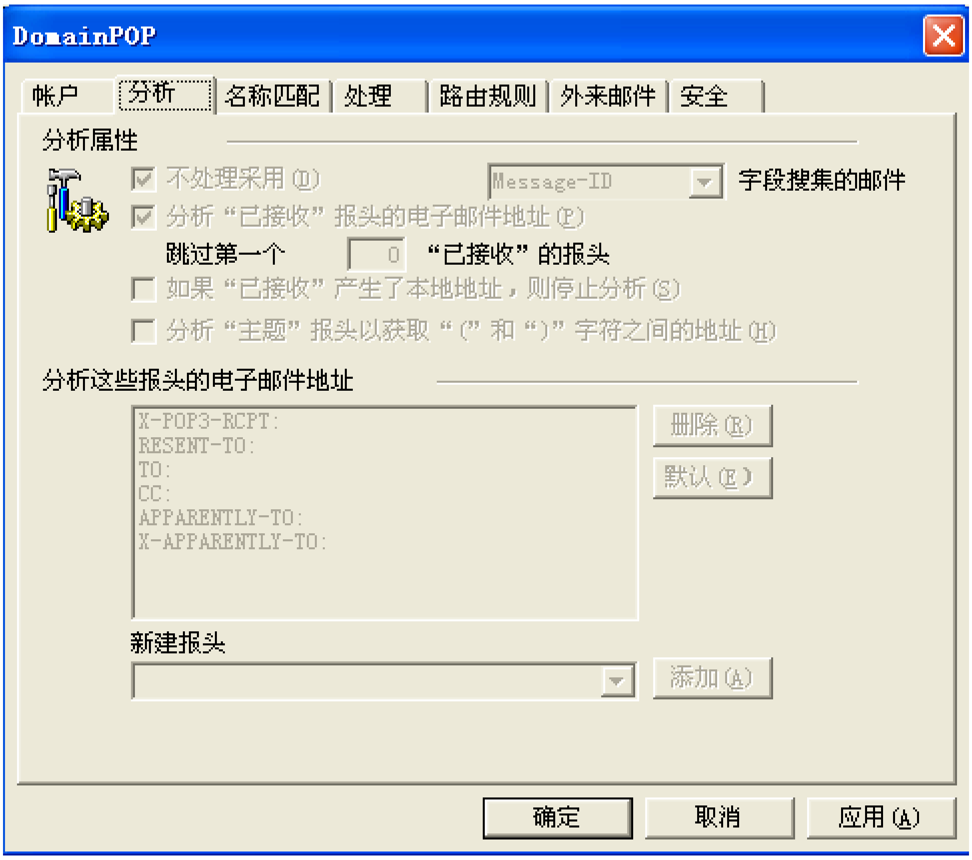
警告帐号持有人，并删除超过限额的邮件

当选择此选项并且为一个超过它配额的帐号收集邮件时（在帐号编辑器的配额标签上指定），MDaemon 将会删除邮件，并发送一个警告到用户，使他们知道他们的帐号超过了它的限制。

警告帐号持有人，并转发超过限额邮件给邮件管理员

当选择此选项并且为一个超过它配额的帐号收集邮件时（在帐号编辑器的配额标签上指定），MDaemon 将会转发邮件给邮件管理员，并发送一个警告到用户，使他们知道他们的帐号超过了它的限制。

分析



分析属性

使用 Message-ID 字段解析收集的邮件，

如果此选项选择，MDaemon 将会记住邮件头中指定的值，并且将不会处理在包含相同值的所收集到的邮件。Message-ID 字段是普通的邮件头，但是实际邮件头可以是你希望的任何字段。

对 E-mail 地址解析 “Received” 邮件头

这个开关可是使用一个强力的几乎不被使用的可选 RFC-822 规则。存储在邮件头中包含的收件人信息来处理邮件，获得一个实际的收件人地址。果你将此开关设置成解析所有合法地址的邮件消息中发现的“received”头，MDaemon 将会尝试利用此可选规则。

跳过最初的 xx “Received” 邮件头

有时，处理 Received 邮件头但从他们的第 n 个开始是非常有用的。此设置允许你输入 MD 将会在开始它的处理前跳过“Received”邮件头的数量。

如果 “Received” 字段包含本地地址，停止解析

如果当解析一个“received”邮件头时，MDaemon 检查到一个合法的本地地址，此开关将导致所有高级解析停止，并且 MDaemon 将不会搜索邮件来查找在的更合适的投递地址。

*解析"**Subject**"邮件头以获取 '(' 和 ')' 字符之间的地址*

当选择此项，MDaemon 在一个邮件的"Subjcet："邮件头中发现了一个含有"()"的地址，此地址将会连同其它解析的地址被添加到收件人的邮件列表中。

为 Email 地址解析邮件头

此控制列出 MDaemon 将会尝试解析提出地址的邮件头。在此所列的每一个邮件头都将被检查来获取地址。

移除

此按钮将从邮件头列表中移出所选条目。

默认

此按钮将会清除当前邮件头列表的内容，并且添加 MDaemon 的邮件头默认列表。默认邮件头具有充分的代表性来从邮件中获取所有地址。

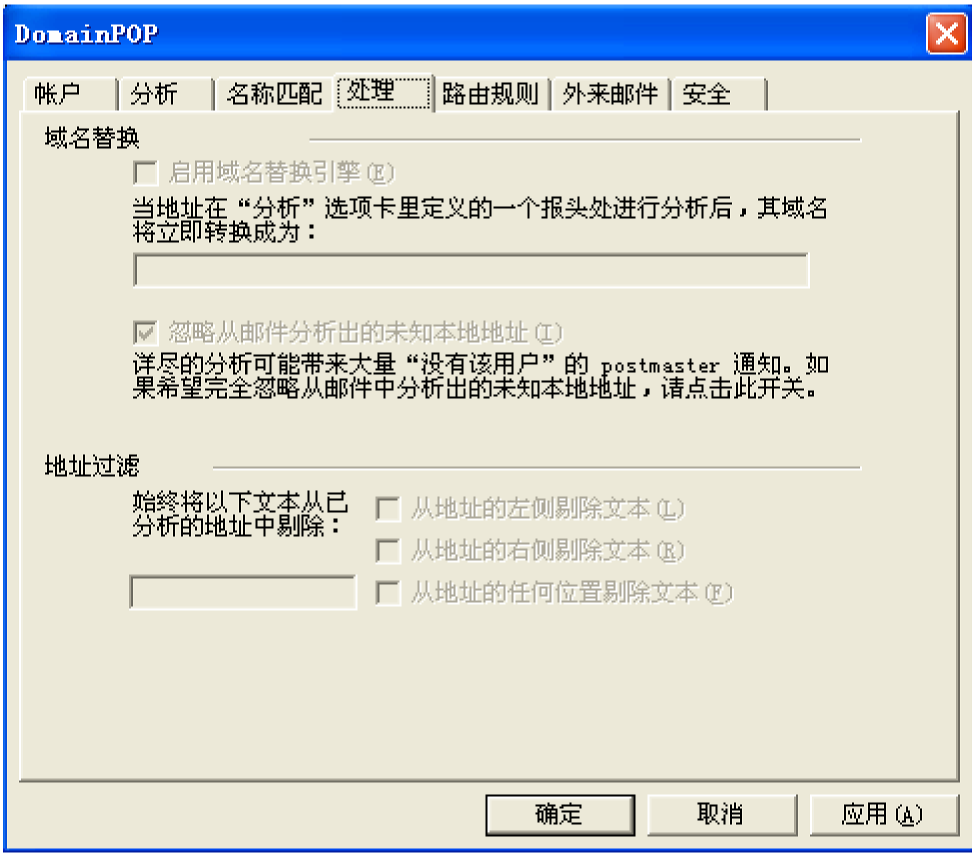
新建邮件头

输入你希望添加到邮件头列表的邮件头

添加

添加在*新建邮件头*控制中所列的邮件头到此列表中。

处理



域名替换

启用域名替换引擎

此选项可以尝试削减你站点将会要求域别名的数量。当下载一封邮件，所有邮件地址所有域名将会立即被转换到此指定的域名。

忽略从邮件解析的未知本地地址

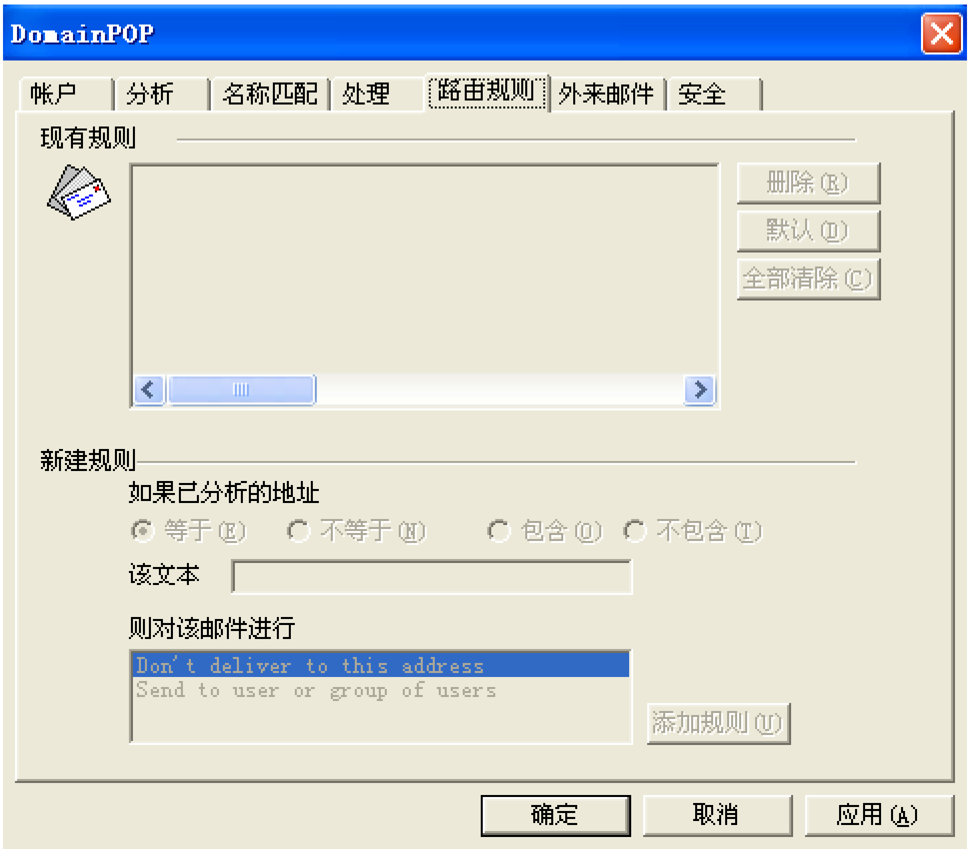
如上面提到的，域名替换功能将会为所有从邮件中解析的邮件地址中更改域名，转换它到一个你指定的。这可能创建一些不与你的站点相匹配的邮箱帐号地址。由于域名将要替换你的主域名，MDaemon 将会考虑此类未定义的本地地址。此类邮件典型的生成一封发往邮件管理员的“无此类用户”消息。这个开关将阻止域名替换引擎生成“无此类用户”消息。

地址过滤

总是从所有解析的地址中去除下列文本

一些 ISP 将会使用一些标记消息连同一点附加地址的路有信息在左侧或者右侧，以指出消息的接收人。此标记对于解析收件人地址是为非常完美的，除了没有大量帐号别名的附加信息使其变得不可能。比作所有的事情强的是，你可以简单的指定与此功能关联的编辑框中的值，并且 MDaemon 将从所有它解析过的地址中除去此文本。

路由规则



现有规则
此列表为你显示你已经创建的，并将应用到你的邮件的规则。

移除
按此按钮，并在存在的规则列表中选择的规则将会被移除。

默认
点击此按钮移除所有存在的规则，并使用一套预设的默认值替换它们。

全部清除
此按钮移除所有存在规则。

新建规则
如果解析的邮件地址...

相于，不等于，包含，不包含
当一个地址同此路由规则比较时，将会生成这种类型的比较。MDaemon 将会在“此文本”区域包含的文本搜索每一个地址，然后基于此设置继续处理– 使地址的全部文本精确匹配，不精确匹配，包含此文档或者不包含？

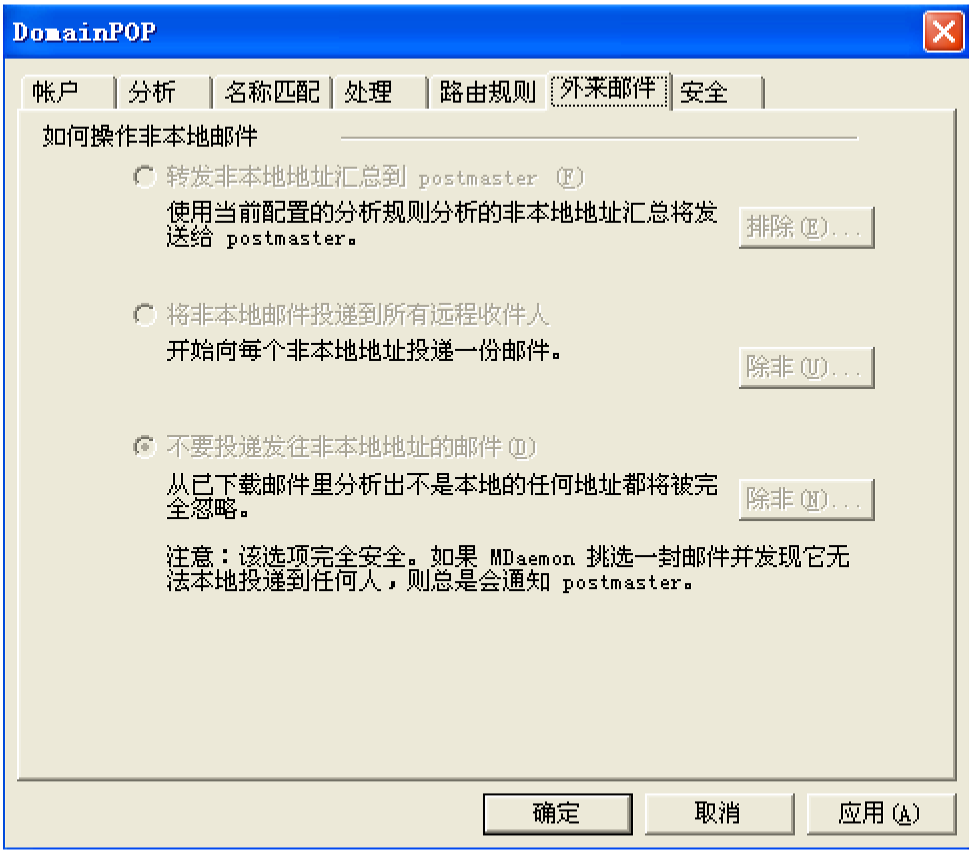
此文本

输入你希望 MDaemon 在检查地址时搜索的文本。

<u>则对该邮件</u>
如果规则的结果为真实的，此控制列出可用的可被执行的操作。这里是操作的列表和它们所做的

Don't deliver to this address – 选择此规则将会阻止消息发送到指定地址。
Send to user or group of users – 选择此操作将会带来一个对话框，并且将允许你创建一个电子邮件列表来接收邮件的副本。

外来邮件



如何处理非本地邮件

转发非本地邮件地址摘要给 postmaster

如果选择了此选项，MDaemon 将会发送一个邮件的副本连同使用当前邮件头设置和解析规则的解析引擎提取出的非本地地址的摘要给 postmaster。

递送非本地邮件到所有远程收信人

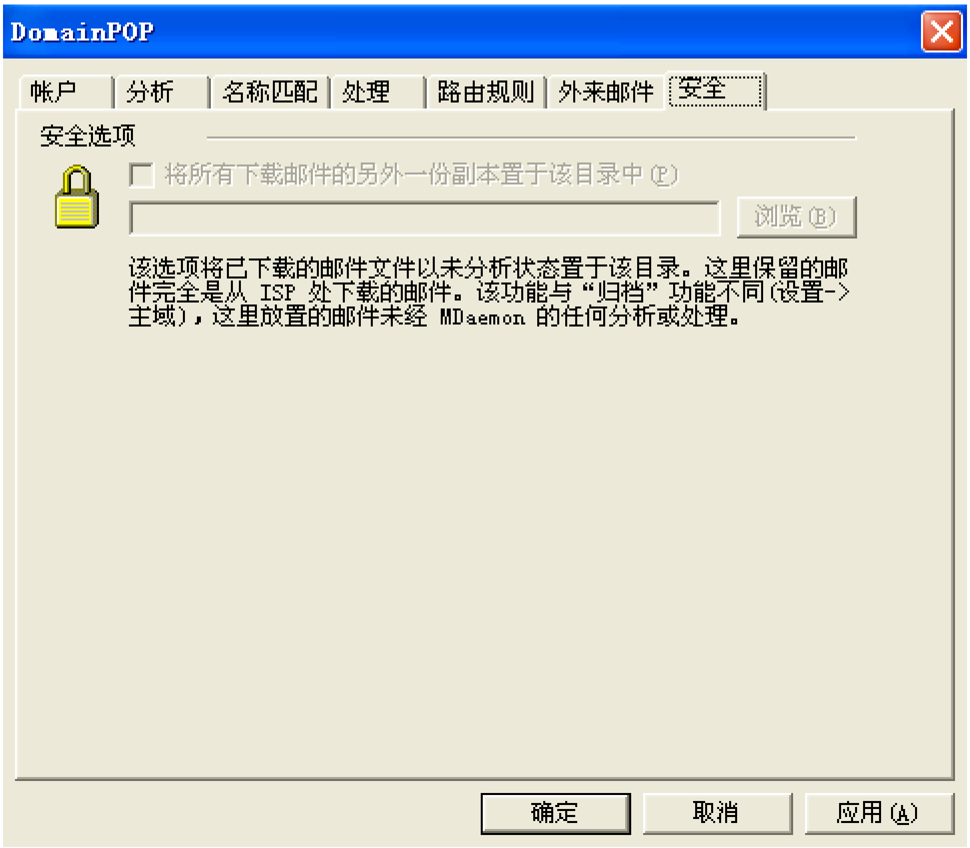
如果选择选项，MDaemon 将会递送邮件的副本给任何在检查的邮件头中找到的非本地收件人。

不递送非本地地址的邮件

如果选择此选项，MDaemon 将会从收件人列表中，移除任何非本地的地址。它就像 MDaemon 从未从原始下载的邮件中解析过远程地址。

注意：
除非..按钮允许你定义在规则之外的地址。

安全

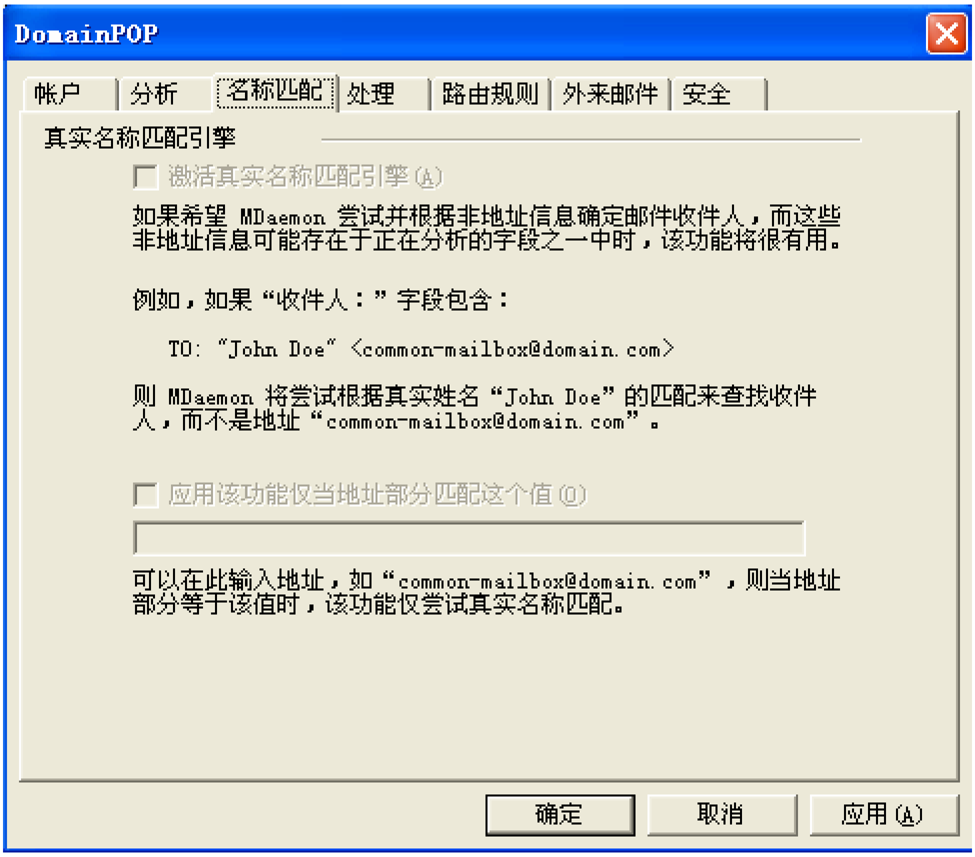


安全选项

所有下载的邮件的额外副本放到此目录

此安全功能保证你不会因为不可预知的解析或者其它可能在垃圾邮件隔离中下载邮件时发生的错误，丢失任何邮件。

名称匹配



注意：

名称匹配功能只有在和 DomainPOP 邮件收集引擎合作的时候才能激活。如果你希望使用此功能，你必须确保你将 DomainPOP 启用。DomainPOP 可以从设置 **– DomainPOP** 菜单选项中开启。

真实名称匹配引擎

激活真实名称匹配引擎

此功能允许 MDaemon 决定谁应该收到一封 DomainPOP 收集的邮件不是基于什么是邮件地址，而是基于文本部分（一个人的全名）是什么。例如来说，一个邮件的 TO 邮件头可能读成：

TO：”Joe User”<common-mailbox@isp.com>

or

TO：Joe User <common-mailbox@isp.com>

名称匹配不在乎地址的 common-mailbox@isp.com 部分。它替换提取”Joe User”部分，并且尝试在 MDaemon 用户数据库中查询此名称。如果在一个帐号的全名区域发现匹配，则此帐号的本地 Email 地址将会用于递送目的。如果没有匹配，则 MDaemon 回复来递送邮件到从数据中解析的 email 地址（此例中的 common-mailbox@isp.com）。

注意：

地址的实名部分不应该包括逗号，引号，冒号，以便你在你的邮件客户端中设置信息时，更好的完成。

如果地址部分匹配此值才应用此功能

此控制允许你指定一个必须在提取出的数据中显示的 email 地址，这是为了全名匹配过程能够继续。这提供你一种在实名匹配被使用时的一种控制方法。例如，你可以指定一个地址为“common-mailbox@isp.com”，然后只有地址匹配此值，才能进行名称匹配。

假设你在此控制中，设置“common-mailbox@isp.com”。

这意味着：

TO: “Joe User” <common-mailbox@isp.com> 将会是名称匹配的后选人，而在TO: “Joe User” <Joe@MDaemon.com> 不是。

第十四章

MDaemon ® 中文版

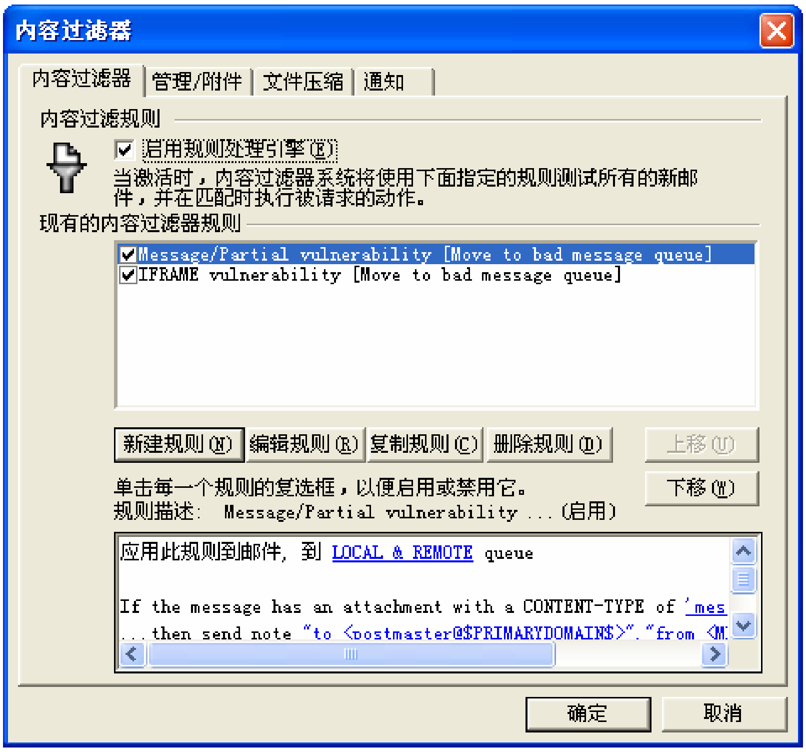
内容过滤器和Anti-Virus

过滤邮件和检查病毒

内容过滤器对话框（安全 – 内容过滤器…）可以有很多用途，比如：在他们到达他们的最终目标前阻止垃圾邮件，截取包含病毒的邮件，复制 email 到一个或者多个额外用户，在文件底部附加一个记录或者拒绝，添加并删除邮件头，去除 email 附件，删除邮件，及更多。由于管理员创建个人内容过滤器规则，并且由于它们的多样性，他们可以在很多情况中使用，并在大多数部分进行限制。

MDaemon 已经整合了对 MDaemon AntiVirus 的支持。Alt-N Technologies，在与世界闻名的 anti-virus 软件开发者：Kaspersky 实验室的合作中，已经开发了 MDaemon AntiVirus，一个与 MDaemon 整合的，可安装的 anti-virus 引擎。当 MDaemon AntiVirus 被安装时，你将看到在内容过滤器对话框上有两个额外的标签。这些标签被用来直接控制插件的功能，以及指定在检测到病毒时，MDaemon 将会采取什么操作。要获得 MDaemon AntiVirus，请访问 www.altn.com。更多使用 MDaemon AntiVirus 的信息，请参见 239 页。

内容过滤器编辑器



所有通过 MDaemon 处理的邮件将在邮件队列临时点上。当内容过滤器启用时，在任意邮件被允许离开对列前，它将首先通过内容过滤器规则被处理。此步骤地结果将决定如何操作此邮件。

注意：

文件名以字母“P”开始的邮件将会被内容过滤过程所忽略。每一个其他的邮件将会通过内容过滤器系统进行处理。一旦处理，MDaemon 将首先更改文件名的第一个字母为“P”。在此种方法中，一个邮件只会通过内容过滤器系统处理一次。

内容过滤规则

启用规则处理引擎

点击此检查框启用内容过滤器。所有通过 MDaemon 处理的邮件在递送前，将会被内容过滤规则进行过滤。

现有的内容过滤器规则

此框列出所有的规则，这是为了他们将会被应用到一个邮件中。这使得你安排你规则以到达一个更高的多功用性级别成为可能。

例如来说：如果你有一个删除所有包括“This is Spam!”这句话邮件的规则，和一个类似的发送这些邮件到 Postmaster 的规则，则将它们放入正确的顺序将会启用这两个规则应用到邮件。假设在此列表中，没有“Stop Procssing Rules”规则更优先的应用到邮件。如果这样，则你使用*上移/下移*按钮来移动“Stop”规则到其他两个下面。现在任何包含“This is Spam!”的邮件将会被复制到 Postermaster，然后删除。

注意：
MDaemon 有能力创建用于执行多任务并使用与/或逻辑的规则。考虑到以上的例子，你可以创建一个能够完成那些所有及更多任务的规则，来替换使用多个规则。

新建规则
点击此按钮来创建新内容过滤器规则。这将打开设置新规则对话框。

编辑规则
点击此按钮打开在编辑器中的选择的规则。

复制规则
点击此按钮拷贝选择的内容过滤器规则。将会创建一个同样的规则，并添加到此列表中。新规则将会被赋予叫做“Copy of [Original Rule Name]”的默认名称。如果你希望创建多个类似的规则，这是非常有用的。你可以创建一个单独的规则，然后拷贝它们几次，然后根据需要调整这些副本。

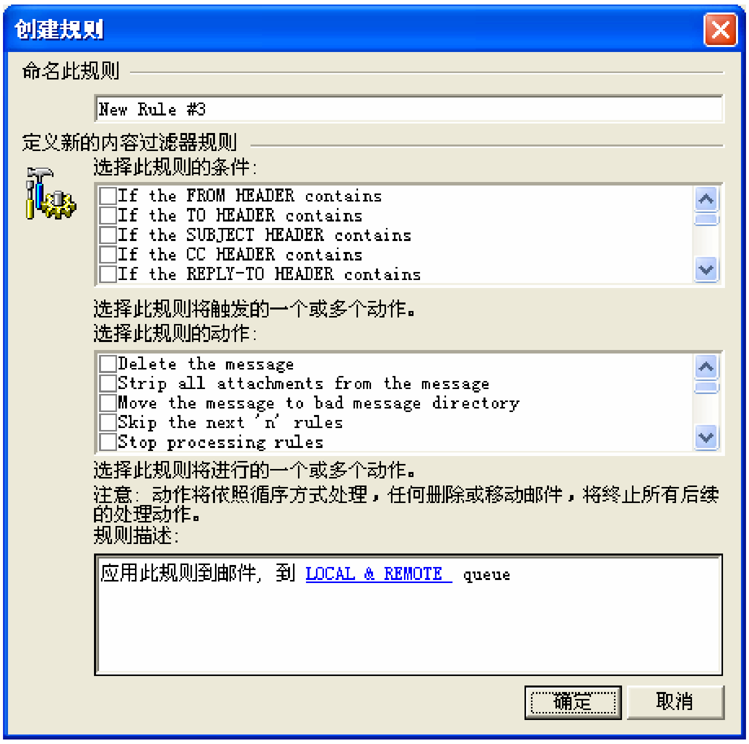
删除规则
点击此按钮删除选择的内容过滤器规则。在 MDaemon 这么做之前，你将被要求确认你的决定来删除规则。

上移
点击此按钮上移所选规则。

下移
点击此按钮下移所选规则。

规则描述[*规则名称*]（启用/禁用）
此框以其内部脚本格式显示当前选择的条目。点击此规则的任何条件（以超链接列出），会打开编辑器来更改详细的设置。

创建新的内容过滤器规则



此对话框用来创建内容过滤器规则。可以通过点击在内容过滤器对话框上的*新建规则*按钮来创建。

命名此规则

在此，为你的新规则输入一个描述性的名字。默认名称为“New Rule #n”。

定义新内容过滤器规则

选择此规则的条件

此框列出可能应用到你的新规则中的条件。点击此复选框中相应的任意你希望应用到新规则的条件。每一个启用的条件将会出现在下面的规则描述框中。大多数条件需要附加信息，这些信息你需要通过点击在规则描述框中的条件的超链接来指定。

If the [HEADER] contains – 点击这些选项的任意一个来创建基于你规则指定的邮件头内容。你必须指定检查的文本。此条件现在支持规则表达。参看“在你的过滤器规则中使用规则表达”。

If the user defined [# HEADER] Contains –点击这些选项的任意一个来创建基于你规则指定的邮件头内容。你必须指定新邮件头，并且指定检查的文本。此条件现在支持规则表达。参看“在你的过滤器规则中使用规则表达”。

If the MESSAGE BODY contains – 此选项将邮件主体内容作为条件之一。此条件要求你指定检查的文本字符串。此条件现在支持规则表达。参看“在你的过滤器规则中使用规则表达”。

If the MESSAGE has Attachment(s) – 当选择此选项，规则只扫描一个或者多个邮件附件。不需要附加信息。

If the MESSAGE SIZE is greater than – 如果你希望规则基于邮件的大小，点击此选项。此大小指定为 KB。默认值为 10KB。

If the MESSAGE HAS A FILE called – 此选项将会对一个有指定名称的文件附件进行检测。此文件名必须指定。允许*.exe 和 file*.*这类的通配符。

If message is INFECTED… – 当 MDaemon AntiVirus 检测到病毒的邮件，则条件为 TRUE。

If the EXIT CODE from a previous run process is equal to – 如果在你的列表中有一个规则利用 *Run Process* 动作，你可以使用此条件来查找从处理过程指定的退出代码。

If the MESSAGE IS DIGITLLY SIGNED – 此条件应用到已经被数字签名的邮件。此条件不需要更多的信息。

If ALL MESSAGE – 如果你希望规则应用到所有邮件，点击此选项。不需要更多的信息；此规则将会影响除了那些在过去的规则中，应用"停止处理中的规则"或者"删除消息"规则的消息外，操作每一个邮件。

选择此规则的动作

如果一个消息匹配规则条件，MDaemon 则可以执行这些操作。一些动作将要求你将通过在规则描述框中，在动作的超链接上点击来指定的附加信息。

Delete Message – 选择此操作将会使得邮件被删除。

Strip All Attachments From Message – 此操作将会使得所有附件从邮件中被去除。

Move Message To Bad Message Directory – 点击此动作导致一个邮件被移动到坏邮件目录。

Skip n Rules – 选择此动作将导致跳过指定数量的规则。在你可能希望一条规则被应用到某些环境但不应用到其他的这种情况时，这是非常有用的。

例如：你可能希望删除某些含有"Spam"的邮件，但是不删除那些含有"Good Spam"的。为了完成此操作，你可能创建一条删除含有"Spam"的邮件的规则，然后将其放到所有规则之上，陈述为"if the message contains "Good Spam" then Skip 1 Rule"。

Stop Processing Rules – 此操作将跳过所有保留的规则。

Copy Message To Specified User(s) – 使得邮件的一个副本被发送到一个或者多个收件人。你必须指定哪些收件人将收到邮件。

Append Standard Disclaimer – 此操作使得你创建小量文本作为注脚附加到邮件中成为可能。另外的，它可以添加一个文本文件的内容。

例如：你可能使用此规则来包含一个为“This email originated from my company, please direct any complains or questions me@mycompany.com”的表述。

Add Extra Header Item To Message – 此动作将会添加一个额外的邮件头到邮件。你必须指定新邮件头的名称和它的值。

Delete A Header Item From Message – 此动作将会从邮件中移除邮件头。你必须指定你希望删除的邮件头。

Send Note To… - 此动作将会发送一个 email 到特别的地址。你将能够制定收件人，发件人，主题，和小量文本。你也可以配置此动作，附加原始邮件到记录中。

例如：你可能希望创建移动所有包含“This is Spam!”的邮件到坏邮价目录的规则，以及发送记录到一些人，使他们知道完成了此动作的规则。

Remove Digital Signature – 点击此动作使得从邮件中移除数字签名。

Run Process… - 此动作用于在一个邮件到达规则条件时，执行一个主要的程序。你必须指定你希望执行的程序的路径。你可以使用$MESSAGEFILENAME$宏来将邮件的名称传到处理过程，并且你可以指定是否 MDaemon 应该临时或者不确定的延缓它的处理，在它等待处理过程终结时。而且，你可以强制处理过程终结，并且/或者将其运行在一个隐藏窗口。

Send Message Through SMS Gateway Server… - 点击此选项通过一个 SMS 网关服务器发送消息。你必须提供主机或者 IP 地址以及 SMS 电话号码。

Copy Message to Folder… - 使用此选项将邮件的副本放置到指定的文件夹。

Add Line To Text File – 此选项可以使得一行文本被添加到指定文本文件中。当选择此动作，你将指定文件的路径，以及你希望附加到其上面的文本。你可以在你的文本中使用某些 MDaemon 宏，使得内容过滤器动态包含关于邮件的发送者，收件人，邮件 ID，及其他的信息。在“Add Line To Text File”对话框上点击宏按钮显示可使用的宏列表。

Move Message to Public Folders… - 使用此动作使得邮件移动到一个或者多个公共文件夹。

Search and Replace Words in a Header – 使用此选项对指定邮件头检查某些单词，然后删除或者替换它们。当创建此规则，点击在规则描述中“指定信息”链接来打开“邮件头 – 搜索和替换”对话框，在此对话框中，你将指派替换或者删除的邮件头和单词。此动作现在支持规则表达。参看“在你的过滤器规则中使用规则表达”。

Jump to Rule… - 使用此动作立即跳到在列表中更靠下的规则，将跳过所有在此两个规则中的规则。

规则描述

此框显示新规则的内在脚本格式。点击任何规则的条件或者动作（作为超链接列出）并将打开相应的编辑器来指定任何需要的信息。

调整存在的内容过滤器规则

调整一个存在的内容过滤器规则，选择规则，然后点击在内容过滤器对话框上面的编辑规则按钮。此规则将被打开，再在规则编辑器中进行编辑。在此编辑器上的控制和创建规则对话框是一致的。

在你的过滤器规则中，使用规则表达

以前，内容过滤系统只支持对指定文本字符串的搜索。现在，它支持"规则表达"搜索，这是一个更为强大的系统，它使得你搜索文本*式样*成为可能。规则表达包含简单文本和特殊字符的混合，以指出做那种类型的匹配，以及因此可以使你的内容过滤器规则变得更为强大和准确。

什么是规则表达？

一个规则表达（regexp）是由 metacharacter 和文字数字的文本字符，或者"文字的"（abc，123，及其他）混合组合而成的文本模式。此模式用于匹配文本字符串 – 匹配的结果成功或者失败。Regexps 主要用于规则文本匹配和搜索及替换。

Metacharaters 是由有特殊功能并用于规则表达中的特殊字符。在 MDaemon 内容过滤系统中的 Regexp 执行允许以下特殊字符：

\ | ( ) [ ] ^ $ * + ? . < >

Metacharacter	描述
\	在使用一个 metacharacter 前，反斜线将会使得 metacharater 被作为一个文字字符。如果你希望规则表达搜索作为 metacharacter 使用的特殊字符其中的一个，这是非常必要的。例如，为了搜索"+"，你的表达中必须包括"\+"。
|	交替字符（也叫作"or"或者"bar"）在你希望在字符任意一边的表达都匹配目标字符串时使用。在搜索文本串时，Regexp"abc|xyz"将会匹配任何不是"abc"就是"xyz"的发生。
[…]	一组包含在方括号中的字符意味着任何在此组中的字符可能匹配搜索的字符串。包括在方括号中的在字符间的破折号（"-"）表示字符的范围。例如，利用 regexp"[a-z]"搜索串'abc'将会产生 3 个匹配：'a'，'b' 和 'c'。使用表达'[az]'将会只产生匹配：'a'。
^	表示线的开始。在此目标串中，'abc ab a'表达'^a'将会产生一个匹配 – 在目标串中的第一个字符。Regexp'^ab'也将产生一个匹配 – 在目标串中的头两个字符。
[^…]	脱字符号（'^'）紧跟着左方括号（'['）有着不同的意思。它可以用于从匹配目标串中排除在方括号中保留的字符。表达"[^0-9]"指出目标字符中不应该有数字。
(…)	括号影响模式赋值顺序，作为一个用于搜索和替换表达的标记表达。 利用规则表达的搜索的此结果可以被临时保持并且可以用于替换表达中来创建一个新的表达。在替换表达中，你可以包括"&"

	或者"\0"字符，这些将被在搜索时规则表达所发现的下级串所代替。因此，如果搜索表达"a(bcd)e"发现一个下级串匹配，则"123-&-123"或者"123-\0-123"此替换表达将会替换匹配文本"123-abcde-123"。 类似的，你也可以在替换表达中使用特殊符号"\1"，"\2"，"\3"及其他。这些字符只有通过标记表达的结果替换来取代整个下级串匹配。在反斜线后面的数字表示你希望涉及的标记表达（在此情况 regexp 包括多于一个标记表达）。例如，如果你搜索表达"(123)(456)"并且你的替换表达为"a-\2-b-\1"，则匹配下级串将会被替换成"a-456-b-123"，反之替换表达为"a-\0-b"将会被替换成"a-123456-b"。
$	美元标志("$")显示行的结尾。在文本串中，"13 321 123"此表达"3$"将生成一个匹配 – 在串中的最后一个字符。Regexp"123$"也将生成一个匹配 – 在目标串中的最后三个字符。
*	星号表示在一行中，字符到其左侧必须匹配 0 或者字符多次重复。因此，"1+abc"将匹配文本"111abc"和"abc"。
+	类似于星号，"+"号表示在一行中，字符到其左侧必须匹配 1 个或者多个字符的重复。因此，"1+abc"将匹配文本"111abc"而不是"abc"
?	问号("?")表示字符到其左侧必须匹配 0 或者 1 次。因此，"1*abc"将会匹配文本"abc"，并且其将匹配"111abc"的"1abc"部分。
.	句号或者点(".")metacharacter 将匹配任意其他字符。因此，".+abc"将匹配"123456abc"，以及"a.c"将匹配"aac"，"abc"，"acc"及其他。

合格条件和动作

规则表达可以用于任何邮件头过滤器规则条件。例如，任何规则使用"if the FROM HEADER contains"条件。规则表达也可以用于"if MESSAGE BODY contains"条件。

注意：
用于内容过滤器规则条件中的规则表达是大小写不敏感的。大写将不会被考虑。

规则表达可能被用到两个内容过滤器规则动作中："Search and Replace Words in Header"以及"Search and Replace Words in the Message Body。"

注意：
使用在内容过滤规则动作的规则表达中的大写灵敏性是可选的。当在规则的动作中创建 regexp 时，你将使得选项关闭/开启大写灵敏性。

在规则条件中配置 Regexp

配置邮件头或者邮件主体条件使用规则表达：

1. 在创建规则对话框中上，点击相应复选框以加入你希望插入到你的规则当中的，邮件头或者邮件主体条件。
2. 在创建规则对话框最下面的总结区域，点击与此条件相应的你在步骤 1

中选择的“**contains specific strings**”链接。这将打开指定搜索文本对话框。
3. 在“当前指定的字符串…”区域，点击“**contains…**”链接。
4. 从下拉列表框中选择“**Matches Regular Expression**”，然后点击**确定**。
5. 如果你需要帮助创建你的 regexp 或者希望测试它，则点击“**测试正规表达式**”。如果你不需要使用测试规则表达对话框，则输入你的 regexp 到提供的文本框中，点击**添加**，然后跳到步骤 8。
6. 输入你的规则表达到“搜索表示式”文本框。简单化处理过程，我们已经提供了一个快捷菜单，可以用来方便的插入希望的特殊字符到你的 expreg。点击“>”按钮进入此菜单。当你从此菜单中选择一个选项，它相应的特殊字符将会被插入到表达中，并且文本插入点将被移动到字符需要的合适的地方。
7. 在提供的文本区域，输入任何你希望用来测试你的表达的文本，并点击**测试**。当你完成对你的表达的测试时，点击确定。
8. 点击确定
9. 继续正常的创建你的规则。

在规则动作中配置 Regexp

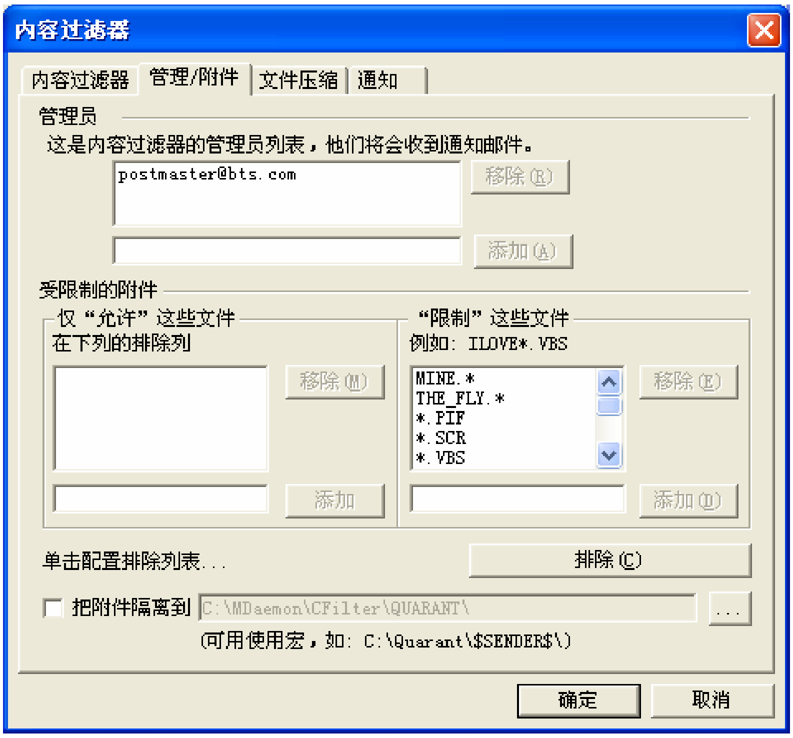
配置一个“Search and Replace Words in…”动作使用规则表达：

1. 在创建规则对话框中上，点击复选框以加入你希望插入到你的规则当中的，“Search and Replace Words in…”相应动作。
2. 在创建规则对话框最下面的总结区域，点击与此动作相应的你在步骤 1 种选择的“**specify information**”链接。这将打开指定搜索文本对话框。
3. 如果你在第一步中选择了“Search …header”，则使用提供的下拉列表框来选择你希望搜索的邮件头头，或者在框中输入邮件头，在希望的邮件头没有在列表中出现的情况下。如果你在步骤 1 中没有选择“Search …header”，则跳过此步骤。
4. 输入你希望在此动作中使用的搜索表示式。简单化处理过程，我们已经提供了一个快捷菜单，可以用来方便的插入渴望的特殊字符到你的 expreg。点击“>”按钮进入此菜单。当你从此菜单中选择一个选项，它相应的特殊字符将会被插入到表达中，并且文本插入点将被移动到字符需要的合适的地方。
5. 输入你希望在此动作中使用的替换表达式。就像搜索表示式，我们现在为此选项也提供了一个特殊字符快捷菜单。如果你希望删除一个匹配的下级串而不是用更多地文本替换，则留此文本框为空。
6. 如果你希望表达式对大小写敏感，点击“**大小写匹配**”。
7. 如果你希望搜索和替换被作为规则表达，则点击“**正规表达式**”。否则其将被作为一个简单的下级串搜索和替换 – 它将对文本的额外的文字匹配进行查找，而不是将其作为规则表达处理。
8. 如果你不需要测试你的表达，则跳过此步。如果你需要测试你的表达，则点击“**运行测试**”。在搜索和替换测试者对话框，输入你的搜索和替换表达，以及你希望测试的文本，点击**测试**。当你完成你的 regexps 时，点击**确定**。
9. 点击**确定**。

10. 继续正常的创建你的规则。

注意：
对规则表达更全面的关注，请参看 O’Reilly & Associates, Inc.出版的 *Mastering Regular Expressions* – http://ww.oreilly.com/catalog/regex2/

管理/附件



使用此标签指定你希望区分为允许和限制的附件。不被允许的附件将自动从邮件中移除。也有用来指定 email 地址为管理员的部分。管理员部分关联的"发送…到管理员"控制在通知标签上。

管理员

在此区域列出的地址作为管理员，并且与通知标签上的管理员控制相关。当此标签上的管理员选项之一被选择时，这些地址将受到通知邮件。添加一个地址到此部分，输入它到提供的空白处，然后点击添加。移除一个地址，从列表中选择它，然后点击移除。

受限制的附件

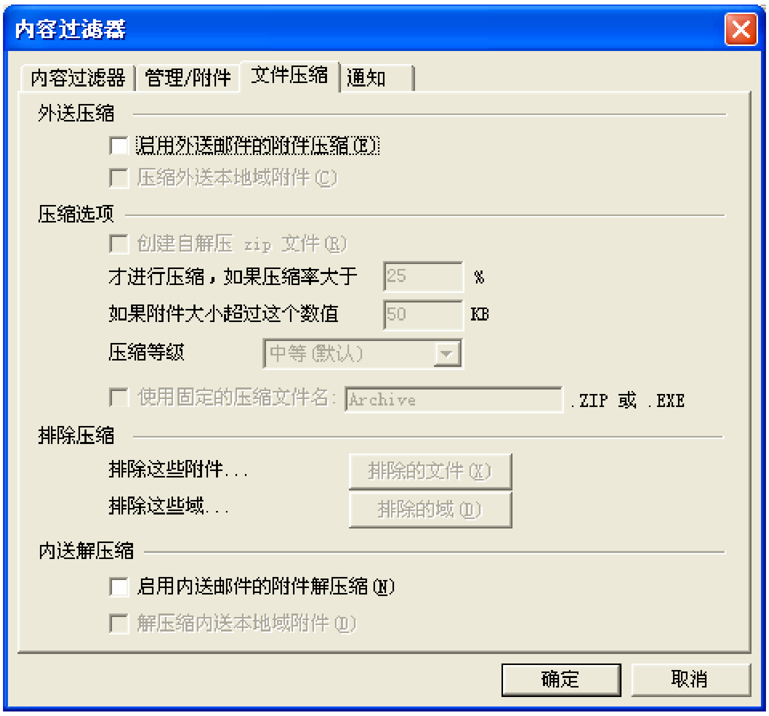
在*受限制的这些文件*列表中指定的文件，在 Mdaemon 处理它们的时候，将从邮件中被自动除去。如果在*仅允许这些文件*...列表中你列出了任何文件，则之后只有那些所列的文件能够获得许可 – 所有其他的附件将从邮件中除去。在附件除去之后，MDaemon 将会正常的继续并递送没有附件的邮件。但遇到这些受限制的附件之一时，你可以使用在通知标签上的控制使得一封通知邮件被发送到不同的地址。

在列表条目中，允许通配符。一个"*.exe"的条目，例如来说，将使得所有以 EXE 文件扩展名结尾的附件被允许或者移除。添加一个条目到任意一个列表，在提供的空白处输入文件名并点击添加。

配置排除

点击*排除*来指定你希望排除在附件限制之外的地址。当从这些地址之一种直接收到一个邮件，MDaemon 将会允许邮件通过，即使它包含一个受限制的附件。

文件压缩



利用在此标签上的控制，在邮件投递前，你可以使得邮件附件自动被压缩或者解压缩。压缩的级别也可以由其他几个参数和例外所控制。此功能可以明显减少带宽的量，以及投递你的外送邮件所需要的吞吐量。

外发压缩

<u>启用外送邮件的附件压缩</u>

如果你希望对外送远程邮件消息，启用自动邮件附件压缩，点击此复选框。启用此控制将不会使所有邮件附件被压缩；它方便的打开此功能。一封外发邮件的文件是否被压缩由此标签上的保留设置决定。

<u>压缩外发本地域附件</u>

启用此控制将会使得文件压缩设置应用到所有外送邮件 – 即使那些文件的最终目标是另外一个本地地址。

压缩选项

<u>创建自解压 zip 文件</u>

如果你希望 MDaemon 创建的压缩文件能够成为有 EXE 文件扩展名的自解压 zip 文件，点击此复选框。如果你顾及到邮件的接收人可能不能访问解压缩软件，则这是非常有用的。自解压文件能够通过双击他们很方便的被压缩。

<u>如果压缩率大于 xx%才进行压缩</u>

在发送邮件前，除非它们能通过高于在此控制中指定值的一个百分比，否则 MDaemon 将不会压缩一封邮件的附件。例如来说，如果你指定此值为 20，并且给定的附件在压缩率至少为 21%前，不能被压缩，然后 MDaemon 将不会再其发送邮件前压缩附件。

注意：
MDaemon 必须首先压缩一个文件来决定它所能被压缩的百分比。因此，此功能不会阻止文件被压缩 – 当它们不能被压缩在指定值之上时，它简单的阻止文件附件以压缩格式被发送。换句话说，如果在压缩文件之后，MDaemon 发现它不能被压缩得超过此值，压缩将被忽视，并且邮件将和它的未作改变的附件一起比递送。

如果附件大小超过这个值 xxKB

当自动附件压缩启用时，MDaemon 将只尝试压缩一封邮件的附件当它们的总大小超过指定值时。附件大小在以下极限的邮件将会和未更改的附件一同被正常发送

压缩等级

使用下拉列表框来选择你希望 MDaemon 应用到自动压缩附件的压缩级别。你可以选择 3 个级别的压缩：最小（最快的压缩处理过程及最差的压缩），中级（默认值），或者最大（最慢的压缩过程，但是最高级别的压缩）。

使用固定的压缩文件名：[archive]

如果你希望自动压缩附件有一个指定文件名，点击此复选框，并且选择一个名称。

压缩排除

排除这些附件…

点击此按钮来指定你想从自动压缩功能中排出的文件。当一封邮件附件匹配这些文件名之一，那么它将不被压缩，无论压缩设置为何。在这些条目中允许通配符。因此，你可以指定“*.exe”，例如来说，并且所有以“.exe”结尾的文件将会保持未压缩状态。

排除这些域…

点击此按钮指定收件人的域，这些域的邮件是你希望从自动压缩中排除的。对这些域的邮件发送将不会把他们的文件附件压缩，无论你的压缩设置如何。

接收解压缩

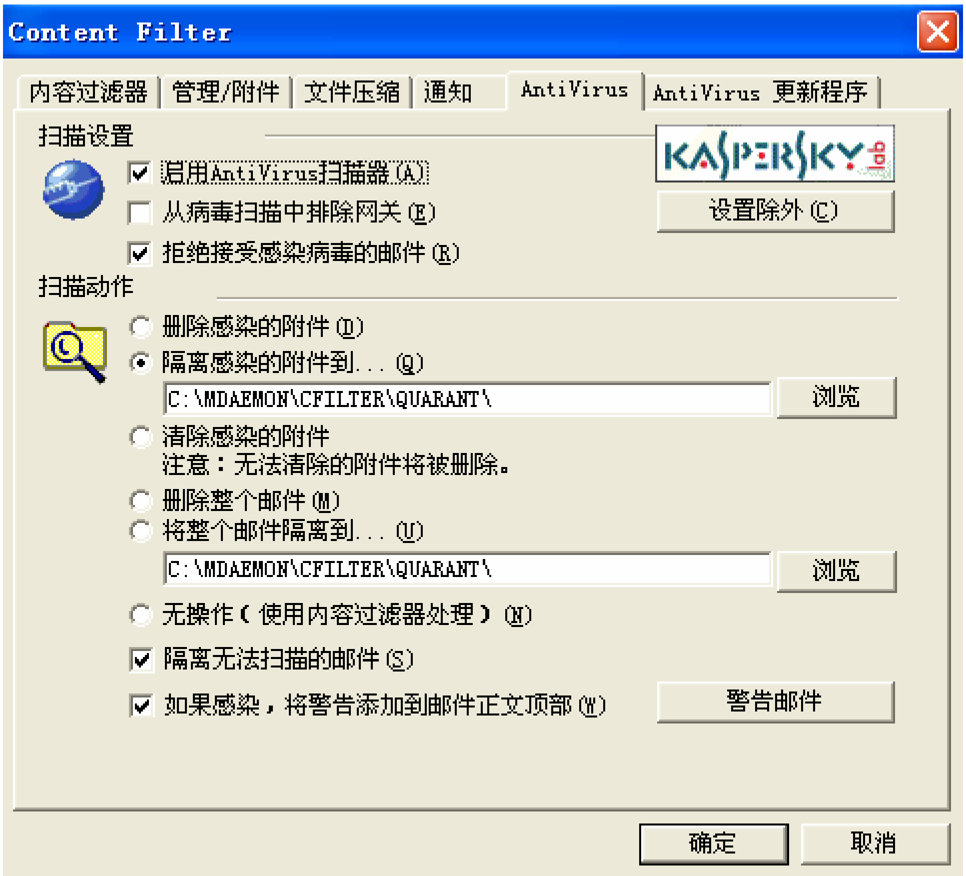
启用接收邮件的附件解压缩

如果你希望启用接收远程邮件消息附件的自动解压缩，点击此复选框。当到达一封含有压缩的附件的邮件时，MDaemon 将会在投递它到本地用户邮箱前压缩它。

解压缩接收本地域附件

如果你希望自动解压缩也应用到本地邮件，启用此控制。

AntiVirus



此标签（以及 AntiVirus Updater 标签）只有在你安装了 MDaemon AntiVirus 后，才可见。获得 MDaemon AntiVirus，请访问 www.altn.com。

扫描器配置

启用病毒扫描器

点击此复选框启用 AntiVirus 邮件扫描。当 MDaemon 收到一封带有附件的邮件时，在递送邮件到其最终目标前，它将激活 MDaemon AntiVirus 并对它们进行病毒扫描。

从病毒扫描中排除网关

如果你希望对 MDaemon 的域网关之一的邮件发送从病毒扫描中被排除，点击此复选框。对于希望将邮件扫描留给域所拥有的邮件服务器来完成时，是非常令人满意的。更多域网关信息，请参看域网关。

点击配置排除列表...配置排除

点击*配置排除*按钮来指定从病毒扫描中排除的收件人地址。对这些地址的邮件发送将不会被 MDaemon AntiVirus 进行病毒扫描。在这些地址中允许通配符。因此你可以使用此功能来排除所有域或者交叉在全部所有域上的特殊的邮箱。例如，“@example.com”或者“VirusArchive@”。

扫描器动作

点击在此部分中的此选项按钮之一来指定 MDaemon 在 MDaemon AntiVirus 检测

到病毒时，将会执行的动作。

删除感染附件

此选项将会删除感染的附件。邮件仍会被递送到收件人，但是将不会有感染的附件。你可以使用在此对话框底部的“添加一个警告…”控制，来添加文本到邮件中，以通知用户受感染的附件已经被删除。

隔离受感染的附件到…

如果你希望受感染的附件被隔离到一个位置，而不是删除或者清除，选择此选项并在提供的空白处指定那个位置。

清除受感染的附件

当选择此选项，MDaemon AntiVirus 将会尝试清除或者停用此受感染的附件。如果附件无法被清除，那么它将被删除。

删除整个邮件

在发现病毒时，此选项将会删除整个邮件，而不仅仅是附件。由于删除整个邮件，“添加一个警告…”选项则将不能应用。但是，你仍可以通过使用通知标签上的控制，发送一封通知邮件给收件人。

隔离整个邮件到…

此选项类似于上面的“删除整个邮件”选项，但是邮件将会被隔离到指定位置，而不是删除。

如果感染，添加一封警告消息到邮件主体顶部

当选择了“…附件”选项之一时，如果你希望在曾经受感染的邮件递送到收件人之前，添加一些警告文本到曾感染的邮件顶部，点击此选项。因此你可以通知收件收件人附件已经被除去，以及为什么这么做。

编辑警告邮件…

当“添加一封警告邮件…”功能被使用时，点击此按钮，显示将会被添加到邮件的警告文本。在对此文本作出任何更改后，点击“OK”来关闭对话框，并保存更改。

AntiVirus 更新程序

使用在此标签上的控制，手动或者自动的更新 MDaemon AntiVirus 的病毒定义。这里有自动更新的时间计划器，报告查看器可使你查看何时以及哪一个更新已经被下载，测试功能用来确认你的病毒扫描正在正常的工作。

扫描器信息

此部分告诉你 MDaemon AntiVirus 是否被安装，如果是的话，将告诉你，你正在运行哪一个版本。它也将列出你最新病毒定义更新的日期。

更新配置

激活紧急更新

点击此复选框激活紧急更新功能。当此功能启用时，AntiVirus 将立即连接更新位置并下载高优先权的更新，无论何时 MDaemon 收到一封"紧急更新"邮件。为了收到这些邮件，你必须首先预订"紧急更新"邮件列表。参看以下的*订阅*控制。

订阅

此按钮打开你的默认浏览器到 Alt-N Technologies 的紧急更新订阅主页。在此页上，输入你的域名称，在紧急更新邮件列表中预订你的域。无论何时有一个对 MDaemon AntiVirus 的病毒定义的紧急更新，一封 email 将会被分发到此域。当 MDaemon 收到邮件时，MDaemon AntiVirus 将会立即更新。

立即更新 AV 定义
点击此按钮手动更新病毒定义。在按下此按钮后，Updater 将会立即连接。

配置更新
点击此按钮打开 updater。Updater 包括三个标签：Updater URLs，连接和代理。

Updater URLs 标签包括 MDaemon AntiVirus 将会连接以检查病毒签名更新的站点列表。你可以从此列表中添加或者移除网站，并且通过提供的箭头按钮，在列表中上移或者下移 URLs；更新的网站被以从上到下的顺序进行检查。点击此控制，"在此 URL 列表中，使用随机开始位置"将会以随机顺序检查站点，而不是以他们所被列出的顺序。

连接标签用来指定你希望在连接更新站点时，MDaemon AntiVirus 使用的 Internet 连接配置文件。"从使用面板中使用 Internet 设置"选项实用你默认的 Internet 设置。"手动设置 Internet 设置"选项和并发的控制可以被用来手动选择一个连接配置文件并且制定它的用户名和密码设置。

代理标签包括用来配置任何 HTTP 或者 FTP 代理设置的选项，你当前的网络配置可能需要这些设置来连接更新站点。

查看更新报告
MDaemon AntiVirus 日志查看器可以通过点*击查看更新报告*按钮来打开。此查看器里除了次数，采取的动作，以及其他关于每个更新的其他信息。

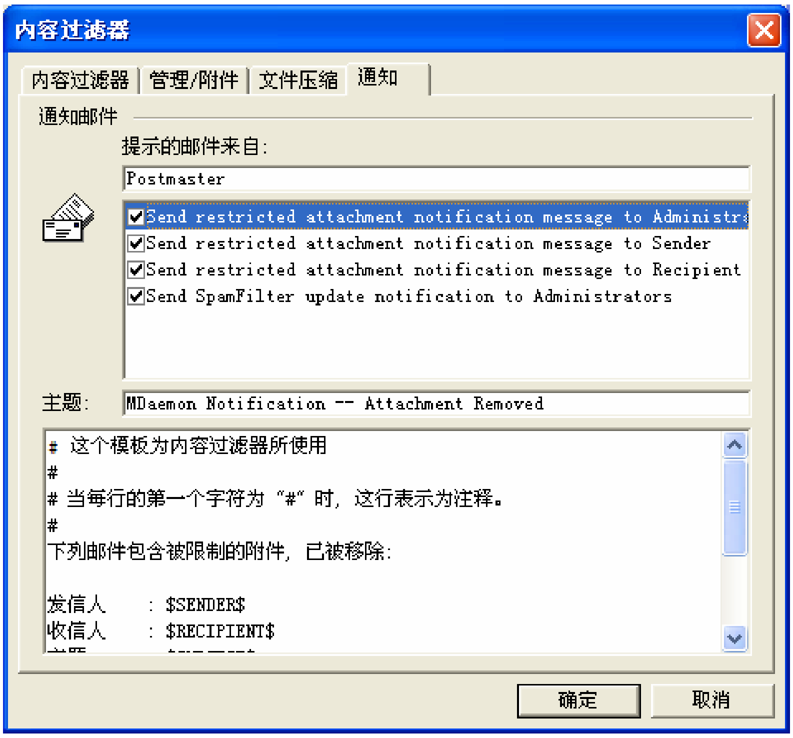
调度程序
点击此按钮，打开 AntiVirus 更新标签上的 MDaemon 的事件日程安排。在此标签上的控制类似于那些在发送&接受邮件标签上的那些控制，并且可以用来安排在指定日期的指定时间进行病毒签名更新，或者通过一个简单的日程安排方法来使的 MDaemon AntiVirus 每一定的分钟一次检查更新。在此标签上也有一个*激活紧急更新*选项，它可以用来激活或者关闭自动紧急更新。此选项与上面所描述的同名控制是一样的。

测试扫描器
发送 EICAR
点击此按钮法发送一封带有EICAR病毒文件作为附件的测试邮件给postmaster。此附件是无害的 – 它仅仅用来测试MDaemon AntiVirus。通过观察在MDaemon的主界面上的内容过滤器的日志窗口，你可以看到在收到邮件时，MDaemon如何操作它的。例如来说，依据你的设置，你可以看到就像以下列出一样的一个日志摘录：

```
Mon 2002-02-25 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2002-02-25 18:14:49: > eicar.com
(C:\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2002-02-25 18:14:49: > Message from: postmaster@mycompany.com
Mon 2002-02-25 18:14:49: > Message to: postmaster@mycompany.com
Mon 2002-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2002-02-25 18:14:49: > Message ID:
```

<MDAEMON10001200202251814.AA1447619@mycompany.com>
Mon 2002-02-25 18:14:49: Performing viral scan...
Mon 2002-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2002-02-25 18:14:50: > eicar.com was removed from message
Mon 2002-02-25 18:14:50: > eicar.com quarantined to C:\MDAEMON\CFILTER\QUARANT\
Mon 2002-02-25 18:14:50: > Total attachments scanned : 1 (including multipart/alternatives)
Mon 2002-02-25 18:14:50: > Total attachments infected : 1
Mon 2002-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2002-02-25 18:14:50: > Total attachments removed : 1
Mon 2002-02-25 18:14:50: > Total errors while scanning : 0
Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@mycompany.com (sender)
Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@mycompany.com (recipient)
Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@mycompany.com (admin)
Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active rules)

通知



当检测到病毒或者受限制附件时，使用此标签指定那些应该收到通知邮件的人。

通知邮件

提示邮件来自:

当一封邮件带着病毒的附件到达时，一封警告邮件将会被发送到在此部分中指定的个人。自定义警告邮件可以被发送到发件人，收件人，以及你在管理/附件标签中已经指定的管理员。为了对此三者的任意之一自定义邮件，从列表中选择他们其中之一，然后编辑出现在此标签中部的邮件。然而每一个条目都有其自己的邮件，尽管在默认值下，由于三者都是一样的，但是这并不明显。

Send restricted attachment notification message to…

当到达一封文件附件的邮件，且此附件匹配受限制附件条目（在管理/附件标签上所列）时，一封警告邮件将会被发送到在此部分指定的个人。一封自定义警告邮件可以被发送到发件人，收件人，以及你在管理/附件标签上已经指定的管理员。为了对此三者的任意之一自定义邮件，从列表中选择他们其中之一，然后编辑出现在此标签中部的邮件。然而每一个条目都有其自己的邮件，尽管在默认值下，由于三者都是一样的，这并不明显。

主题

此文本将在被发送的通知邮件的“主题”邮件头中显示。

邮件

当与此条目相关的复选框被启用时，这是将被发送给在以上列表中所选的条目的邮件。你可以从显示邮件的此框中，直接编辑邮件。

注意：
目前此文件包括在 MDaemon\app\目录中的此文本。它们是： cfattrem[adm].dat 受限制的附件邮件 – 管理员 cfattrem[rec].dat 受限制的附件邮件 – 收件人 cfattrem[snd].dat 受限制的附件邮件 – 发件人 cfvirfnd[adm].dat 发现病毒的邮件 – 管理员 cfvirfnd[rec].dat 发现病毒的邮件 – 收件人 cfvirfnd[snd].dat 发现病毒的邮件 – 发件人 假若你希望将这些邮件中的一个恢复到原始,简单的删除相关文件，MDaemon 将会用其默认表述重新创建它。

邮件宏

为了你的便利，在通知邮件和其他某些内容过滤器生成的邮件中可以使用某些宏。你可以使用以下宏中的任意一个，更多的在 334 页列出：

$ACTUALTO$	一些邮件可能包含“ActualTo”区域，它通常用来表示目标邮箱以及主机，这是因为它是被最初用户优先于任何重定格式或者别名转换前输入的。此宏用来替换所提到的值。
$AV_VERSION$	列出你正在使用的MDaemon AntiVirus的版本。
$CURRENTTIME$	当邮件被处理时，此宏被用来替换当前时间。
$ACTUALFROM$	一些邮件可能包含“ActualFrom”区域，它通常用来表示优先于任何重定格式或者别名转换的原始邮箱以及主机。此宏用来替换所提到的值。
$FILTERRULENAME$	此宏用来替换规则的名称，此邮件匹配规则的标准。
$HEADER:XX$	此宏将导致在“XX”处指定的邮件头的值将被扩展到重定格式的邮件中。例如：如果原始邮件是“TO：joe@MDaemon.com”，则$HEADER:TO$宏将会扩展成为“joe@MDaemon.com”。如果原始邮件是“Subject：This is the subject”，则$HEADER:SUBJECT$宏将会被文本“This is the subject”所替代。
$HEADER:MESSAGE-ID$	和上面的$HEADER:XX$类似，此宏将扩展到Message-ID邮件头值。
$LIST_ATTACHMENTS_REMOVED$	当从邮件中移除一个或者多个附件时，此宏将列出它们。
$LIST_VIRUSES_FOUND$	当在邮件中发现一个或者多个病毒时，此宏将列出它们。
$MESSAGEFILENAME$	此宏扩展到当前正在处理的邮件的文件名。

$MESSAGEID$	除了此宏从message ID值中去除“< >”，其他就像上面的$HEADER:MESSAGE-ID$一样。
$PRIMARYDOMAIN$	扩展到MDaemon的主域名称，可以在主域配置对话框上指定（点击设置 – 主域）。
$PRIMARYIP$	此宏扩展到你的主域的IP地址（在主域配置对话框中指定）。
$RECIPIENT$	此宏解决邮件接收器的所有地址。
$RECIPIENTDOMAIN$	此宏将插入邮件接收器的域名称。
$RECIPIENTMAILBOX$	列出邮件接收器的邮箱（在email地址中，此值在@左侧）。
$REPLYTO$	此宏扩展到邮件的“Reply-to”邮件头的值。
$SENDER$	扩展到从邮件被发送到的所有地址。
$SENDERDOMAIN$	此宏将插入邮件发送者的域名称（在email地址中，此值在@右侧）。
$SENDERMAILBOX$	列出发件人的邮箱（在email地址中，此值在“@”的左侧。
$SUBJECT$	显示在邮件主题中包含的文本。

第十五章

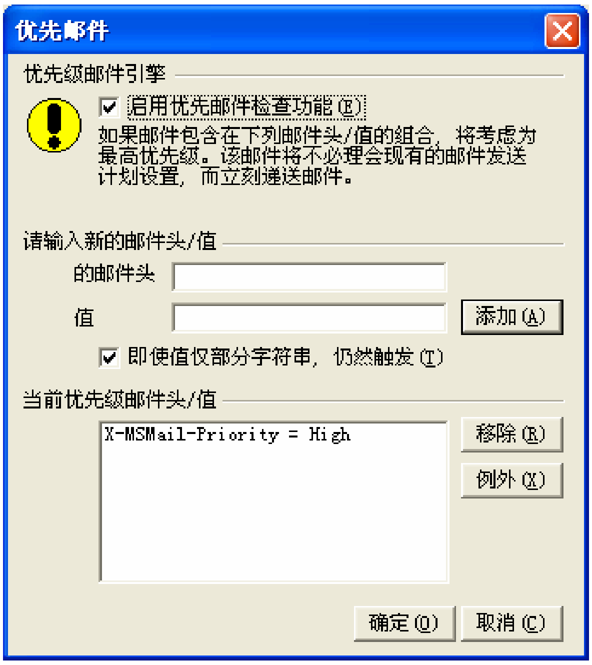
MDaemon ® 中文版

优先级邮件

配置和使用优先级邮件功能

设置 – 优先级邮件...菜单选项打开优先级邮件对话框，它用来定义在你的系统中，由什么来组成你的优先级邮件。优先级邮件将通过 MDaemon 立即被递送，无论如何安排的邮件处理间隔。当到达一封新邮件时，MDaemon 将会对一组你在对话框中已经制定的邮件头/值组合，来检测它的邮件头。如果它发现了它们，它会认为此邮件具有高优先级，并且尝试立即递送它。

优先级邮件



优先级邮件引擎

__启用优先邮件检查功能__

点击此开关启用优先级邮件功能。MDaemon 将会对优先级状态检查来信。

请输入新的邮件头/值

__新的邮件头__

在此区域输入邮件的邮件头。不要包括结尾的句号字符。

__值__

输入的值必须能够在制定的邮件头中找到，这是为了邮件可以被认为成高优先

级。

即使该值仅为部分字符串，仍然触发
当输入一个新的优先级邮件设置，你可能选择此功能来对一个邮件头值的一部分（或者下级串）的启用优先级匹配。例如来说，你可以为带有值“BOSS”的“TO”邮件头创建优先级邮件设置。然后在邮件头中，任何包含“Boss@anything”的 email 都将被认识是优先级邮件。如果创建一个没有启用此功能的条目，则邮件头的值必须精确匹配条目；只匹配一部分将会是不够的。

添加
当在指定的文本框中输入邮件头/值信息后，并且指定是否此条目将会应用到下级串，点击*添加*按钮来创建新的优先级邮件条目。

当前的优先级邮件邮件头/值
此窗口列出所有当前定义的优先级邮件邮件头/值组合。在此列表中的一个条目上双击将移除它。

移除
点击此按钮，从*当前的优先级邮件邮件头/值*窗口中移除一个所选的条目。

例外
这允许你定义将会使邮件被认为是优先级邮件设置的例外的区域/值组合。这将在此功能基础上赋予你更多的灵活性。

第十六章

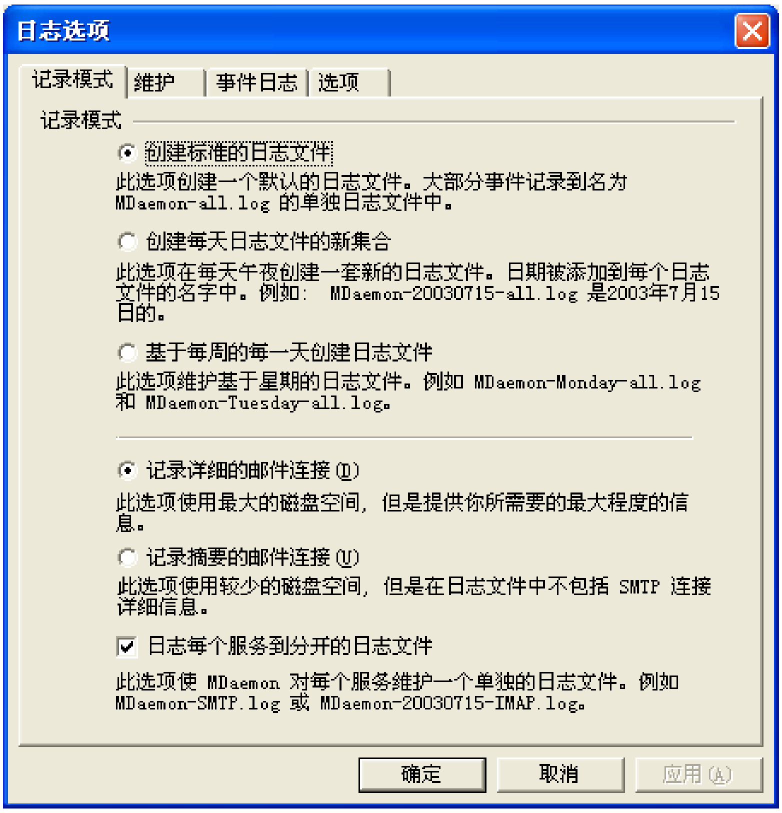
MDaemon ® 中文版

日志

配置**MDaemon**的日志选项

点击**设置 – 日志…**菜单选项（或者按 **Alt+F7**）来配置你的日志选项。日志对诊断问题以及查看服务器在未被照看时，都作了哪些工作，是非常有用的。

日志模式



注意：
在其他选项对话框上管理日志数据量的几个控制可以显示在 MDaemon 的主界面的路由窗口中。更多信息，参看其他选项 – GUI。

日志模式

<u>创建标准的日志文件</u>

点击此选项生成一个标准的单独的日志文件。

<u>创建每天日志文件的新集合</u>

如果选择了此选项，则每一天都将创建单独的日志文件。文件的文件名将会和他们创建的日期相关。

基于每周的每一天创建日志文件

如果选择此选项，则此周的每一天都将创建单独的日志文件。文件的文件名将会和他们创建的那周的日期相关。

记录详细的邮件链接

当此选项激活时，每一个邮件处理会话的一份抄本将会被复制到日志文件中。

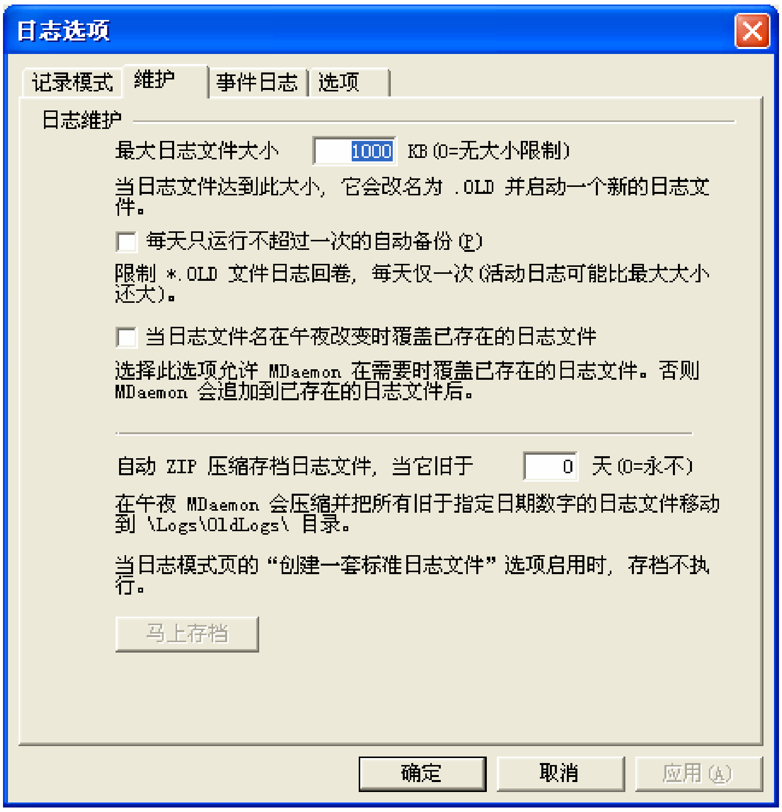
记录摘要的邮件连接

此选项将会使的每一个邮件处理会话的总结性抄本被复制到日志文件。

日志每个服务到分开的日志文件

点击此复选框，使得 Mdaemon 基于服务生成分开的日志，而不是在一个单独的文件中。例如来说，利用此开关设置 MDaemon 在 MDaemon-SMTP.log 文件中将会记录 SMTP 活动，以及在 MDaemon-IMAP.log 文件中记录 IMAP 活动。当你运行一个“ghost”或者 MDaemon 终端服务试，必须选择此选项，这是为了在界面上的标签可以显示记录信息

维护



<u>最大日志文件大小[xx]KB</u>

这是日志文件可以到达的最大文件大小，以 KB 为单位。一旦达到了此大小，日志文件将被复制到 LOGFILENAME.OLD，并且开始一个新日志。

<u>每天只运行不超过一次的自动备份</u>

当限制日志文件大小时，如果你希望每天备份不超过一个日志文件，点击此检查框。每天，日志文件第一次达到最大大小时，他将被更名为“*.OLD”并被正常保存。后来的日志文件将会继续变大，无论如何指定最大大小。直到下一天前，它将不会被滚动 – 即使超过了最大大小设置。

<u>当日志文件名在午夜改变时覆盖已存在的日志文件</u>

通过默认值，当 MDaemon 在午夜更改日志文件名，并且它所改变的文件名已经存在时，它将添加新的记录信息到已存在的文件。例如，如果 MDaemon 更改 Monday.log 为 Tuesday.log，并且名字为 Tuesday.log 的文件已经存在，那么它将添加新的记录数据到已存在的文件中，而不是覆盖它或者创建一个新的。如果你希望 MDaemon 覆盖任何已经存在的文件，而不是添加新的数据到其中，点击此复选框。

*<u>自动 **ZIP** 压缩存档日志文件，当它旧于 **xx** 天（**0=**永不）</u>*

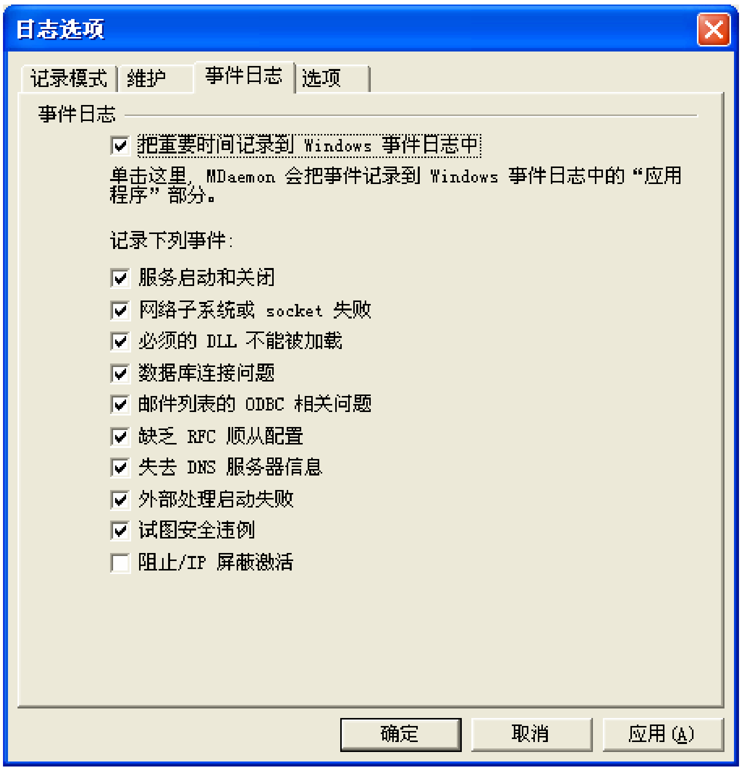
如果你希望 MDaemon 存档每一个超过指定天数的日志文件，点击此选项。每天午夜，MDaemon 将会压缩旧的*.log 和*.old 文件，并且把他们移动到\Logs\OldLogs\下级文件夹中（删除处理过程中的原始文件）。此处理过程将不会

存档或者删除正在使用的文件，当选择在日志模式标签上的“创建标准日志文件”选项时，也不会存档。

马上存档

点击此按钮立即存档旧的日志文件，而不是等待 MDaemon 在午夜自动存档它们。

事件日志



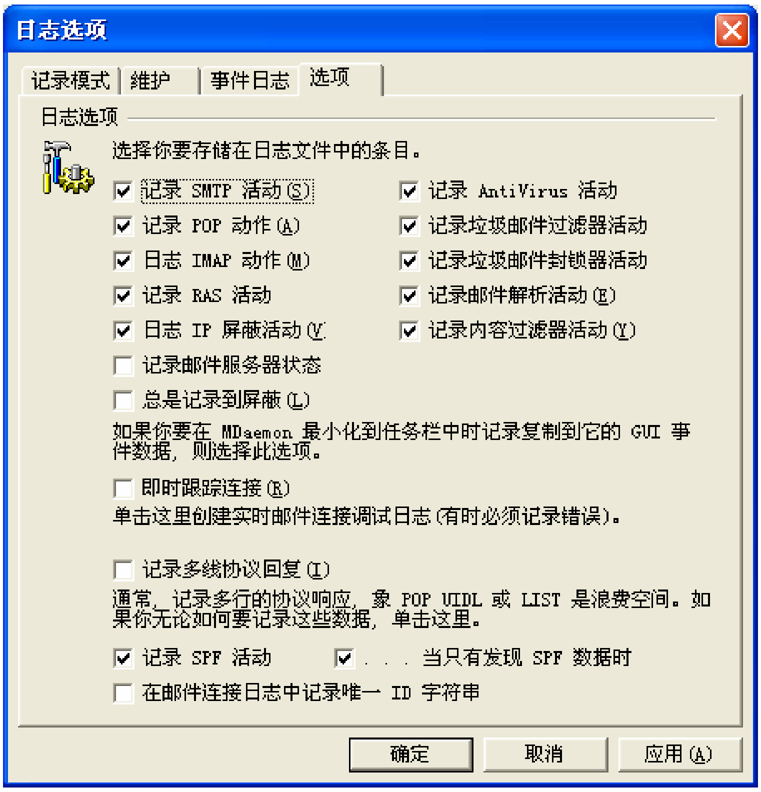
<u>把重要时间记录到 Windows 事件日志中</u>

如果你希望跟踪危急的系统错误和警告，点击此复选框。

<u>记录下列事件：</u>

如果你记录 Windows 事件，使用此组选项来指定你希望记录哪些事件。

选项



日志选项

<u>记录 SMTP 活动</u>

如果你希望记录所有 MDaemon 发送/接受的 SMTP 活动，点击此选项。

<u>记录 POP 动作</u>

点击此复选框记录所有 POP 邮件活动。这将从 MDaemon 记录你的用户的 POP 邮件收集会话，并且将记录 MDaemon 的 DomainPOP 以及 MultiPOP 活动。

<u>记录 IMAP 动作</u>

启用此选项将会使得所有你的用户的 IMAP 会话被包括在 MDaemon 的日志文件中。

<u>记录 RAS 活动</u>

如果你希望 MDaemon 复制 RAS 拨号/挂断活动到日志文件中，点击此复选框。此信息对于诊断拨号问题是非常有用的。

<u>记录 IP 屏蔽活动</u>

如果你希望 IP 屏蔽活动被包括在 MDaemon 的日志文件中，点击此复选框。

<u>记录邮件服务器状态</u>

由于日志文件的统计可能在维护的时候，使用大量磁盘空间和 CPU 效用。此选项可以使得你控制是否创建那个文件成为可能。此开关默认状态下是关闭的。

记录 AntiVirus 活动
此选项记录 MDaemon AntiVirus 活动

记录垃圾邮件过滤器活动
记录所有垃圾邮件过滤器活动。

记录垃圾邮件封锁器活动
此选项是 MDaemon 记录垃圾邮件封锁器活动。使用此选项将会允许你拥有对被记录为黑名单的站点的简单参考。

记录邮件处理活动
当决定一封邮件递送的目标时，MDaemon 周期性的执行大量的邮件处理活动。如果你希望此信息被包括在日志文件中，点击此选项。

记录内容过滤器活动
如果你希望包含内容过滤器和 MDaemon AntiVirus 活动在日志文件中，点击此复选框。

总是记录到屏幕
如果你希望记录数据被复制到 MDaemon GUI，即使当 MDaemon 最小化或者以托盘方式运行时。

当清空此控制室，记录数据将不能在 MDaemon 以系统托盘方式运行时，复制到路由窗口。因此，在 MDaemon 首次被打开时，大多数最近的活动将不会被列到任何路由窗口的标签上。路由器将从那一点向前，开始显示新的记录信息。

实时记录连接
通常，会话信息将在会话完成后被记录，这是为了保存资源。如果你希望会话信息当在发生中被记录，点击此选项。

记录多线协议响应
有时，对协议请求的回应要求多于一线的信息。如果你希望记录这些附加线，点击此复选框。

小心：
启用此控制可能潜在的大量增加记录信息的量。由于在回应中的线的数量不能预先决定，并且由于一些回应会前在的使用可能不重要的信息填满你的日志文件（例如，那些列出邮件真实内容的 POP TOP），因此，如果你关注冗长的日志文件大小，那么我们不推荐使用此功能。

记录 SPF 活动
如果你希望记录所有 SPF 查找活动，点击此选项。

…当只有发现 SPF 数据时
如果你记录 SPF 活动，在你希望只记录在 DNS 查询中发现的记录，而不是记录

所有 SPF 查找时，点击此复选框。

在邮件连接日志中记录唯一 ID 字符串

如果你希望包括[%d:%d]唯一 ID 字符串在会话记录中，点击此选项。

第十七章

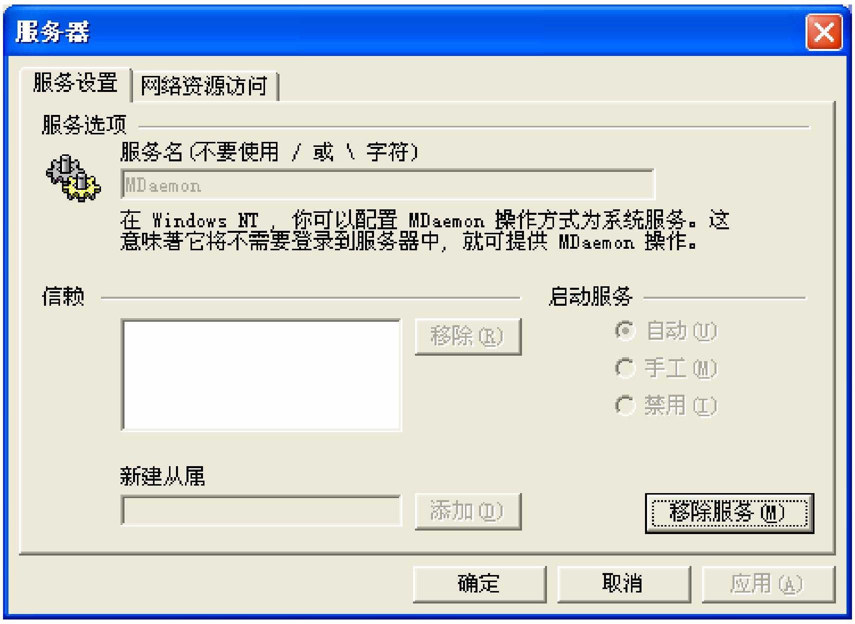
MDaemon® 中文版

系统服务设置

作为一个系统服务运行MDaemon

使用**设置 – 系统服务...**菜单选项(或者按 Alt+F8)来打开你可以在 Windows NT/2000/XP 下配置 MDaemon 作为一个系统服务运行的对话框。如果你运行在 Windows 9X 中，你将看到一个和 NT/2000/XP 不同的系统服务对话框。尽管不复杂，但是在 Windows 9x 中的服务将仍允许你在没有任何人登陆的情况下处理软件。

服务设置



服务选项

服务名

这是 NT 将会为服务使用的名称。

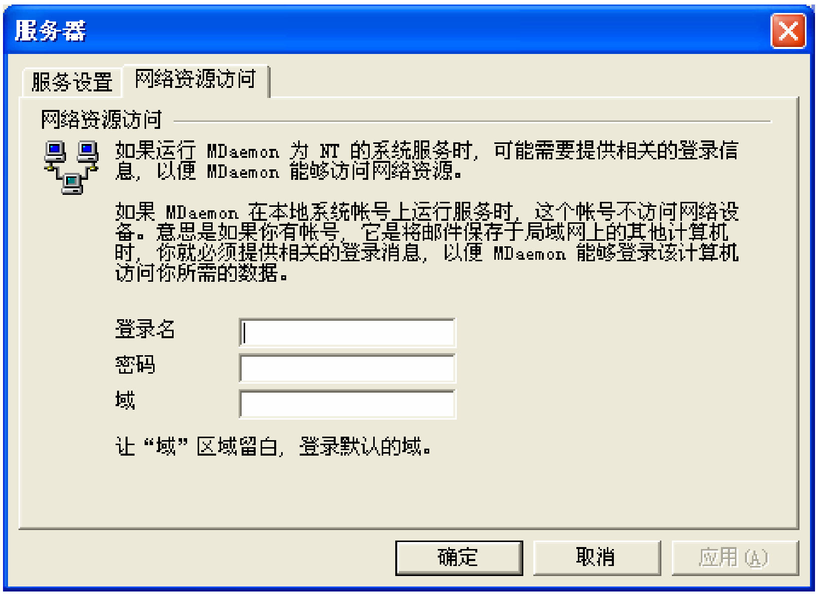
启动服务

这是服务的初始状态。

依赖

MDaemon 服务被尝试载入前，此列表的服务必须在处于激活状态。

网络资源访问



当运行 MDaemon 作为 NT/2000 的系统服务时，通过默认值，它将在本地系统帐号下运行。由于此帐号不能访问网络服务，因此如果你希望在穿过你的 LAN 的其它计算机上存储邮件，MDaemon 将不能访问邮件。更确切的说，并不是除非你提供一个账户登陆证书，此帐号可以用来提供 MDaemon 服务访问网络共享才可以。我们推荐，创建一个为运行 MDaemon 特别设计的用户帐号，并且你可以附加任何你希望的限制，而不是连入那些你希望 MDaemon 可以使用的那些网络共享的那一个。这种方法，你可以在将 MDaemon 作为一个服务运行时，使用 UNC 符号或者映射驱动访问网络共享。而且，所有通过 MDaemon 启动的应用程序（等同于 MDstats 和预处理效用）将也可以使用与此相同 NT 帐号的安全承接关系。

<u>登录名</u>
这是 NT 帐号的登录名，MDaemon 服务应该运行于此帐号下。

<u>密码</u>
这是 NT 帐号的密码。

<u>域</u>
这是帐号所存在的域。将区域的空白处留空，可以登录到默认的域。

第十八章

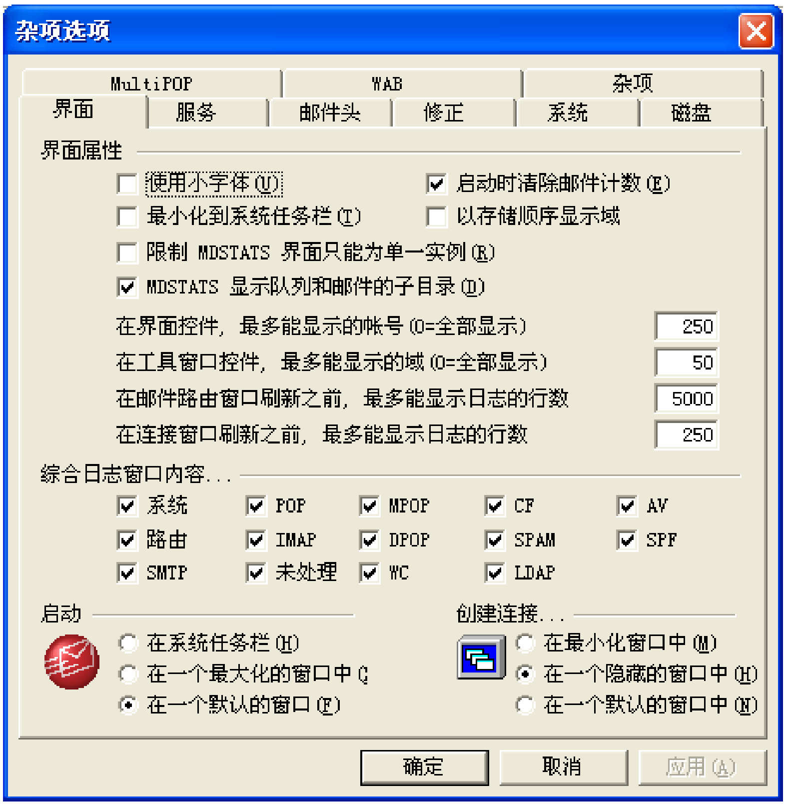
MDaemon ® 中文版

其他选项

MDaemon的其他选项设置

使用设置 – 其他选项…菜单选项来编辑不同的全局设置，设置 SMTP 邮件大小限制，配置磁盘空间监测，以及指定服务器开始和邮件会话的默认窗口的大小。

界面



注意：
在此标签上的控制不会影响实际存储在日志文件中的数据量 – 他们只影响在 MDaemon 主界面的路由窗口中显示的信息。

界面属性

使用小字体

在路由和会话窗口上，启用小字体。

启动时清除邮件计数
当此复选框启用，无论何时启动 MDaemon。在主路由窗口上显示的邮件统计信息将会被重置。
最小化到系统任务栏
当启用此控制，并且 MDaemon 最小化时，它将同时出现在任务栏和系统托盘中。如果你不希望 MDaemon 在程序最小化时，出现在 Windows 托盘中，清空此选项；只有托盘图标可见。

以排列顺序显示域
点击此选项使得在 MDaemon 的主界面上的工具菜单中的域列表可以按字母顺序排列。如果你清除此选项，域将以他们在位于 MDaemon 的\app\目录的 domains.dat 文件中的顺序排列。当此更改此设置时，新的排列顺序将不会反映在界面上直到你重启服务器或者打开并关闭次域对话框。

*限制 **MDstats** 界面只能为单一实例*
如果你不希望多于一个的 MDaemon 的队列和统计管理器在一次运行，点击此复选框。当 MDstats 已经正在运行时，尝试启用 MDstats 将会使得当前运行的实例变成活动窗口。

***MDstats** 显示队列和邮件的子目录*
如果你希望队列统计管理器显示在不同队列以及用户邮件目录中包含的下级文件夹，点击此选项。

*在界面中，最多能显示的帐号（**0**=全部显示）*
这是将在不同的对话框的下拉列表框中显示的最大数量的帐号。而且，当在此控制中的值设置为其他非“0”（全部显示）时，“编辑帐号”和“删除帐号”选项将不再出现在帐号菜单上。那些功能将只在帐号管理器上可用。在对此控制的任何更改生效前，你必须重启 MDaemon。

*在工具窗口控件，最多能显示的域（**0**=全部显示）*
这是在主显示的工具窗口中的“服务器”控制下所列的次域的最大数量。在更改此值后，在工具窗口中更改生效前，你必须按 F5 或者重启 MDaemon。此控制不能设置成为任何超过 50 的值。

在邮件路由窗口刷新之前，最多能显示日志的行数
这是在主显示的日志窗口中显示的最大数量的行数。当达到此数量的行，窗口将被清空。这对日志文件没有任何影响。只有显示将被清空。

在连接窗口刷新之前，最多能显示日志的行数
这是在每一个会话连接窗口被清空前，将在其里面出现的最大数量的行数。这对日志文件没有任何影响。

综合日志窗口包括**…**
位于 MDaemon 的菜单栏的窗口菜单上的是组合日志查看选项。点击此选项将会

添加一个窗口到将会把在一个或者多个路由器标签上显示的信息组合的路由器中。使用此部分中的此控制指定哪一个标签的信息将会组合到那个窗口中。在以下的标签中包含的信息将会被组合：

系统	显示 MDaemon 的系统活动，比如初始服务以及启用/停用任何 MDaemon 的各种服务器。
SMTP	显示所有使用 SMTP 协议的发送/接受会话活动
IMAP	记录使用 IMAP 协议的邮件会话。
DPOP	显示 MDaemon 的 DomainPOP 活动。
路由	显示通过 MDaemon 解析的每一个邮件的路由信息（To，From，Message ID，以及其他）。
POP	当用户从使用 POP3 协议的 MDaemon 中收集邮件时，记录此活动
未处理	RAW 或者系统生成的邮件活动将被记录。
MPOP	显示 MDaemon 的 MultiPOP 邮件收集活动。
CF	MDaemon 的内容过滤器处理将被列出。
AV	AntiVirus 处理将显示在组合查看中。
SPAM	显示所有垃圾邮件过滤活动。
SPF	显示所有发件人策略层活动。

启动

在系统任务栏

如果你希望 MDaemon 的界面在开始时最小化，选择此选项。

在一个最大化的窗口中

如果你希望 MDaemon 的界面在开始时最大化，选择此选项。

在一个默认的窗口

如果你希望 MDaemon 的界面在开始时出现在默认的窗口中，选择此选项。

创建连接

在最小化窗口中

如果选择此选项，MDaemon 将会以最小状态创建一个新的邮件连接窗口。

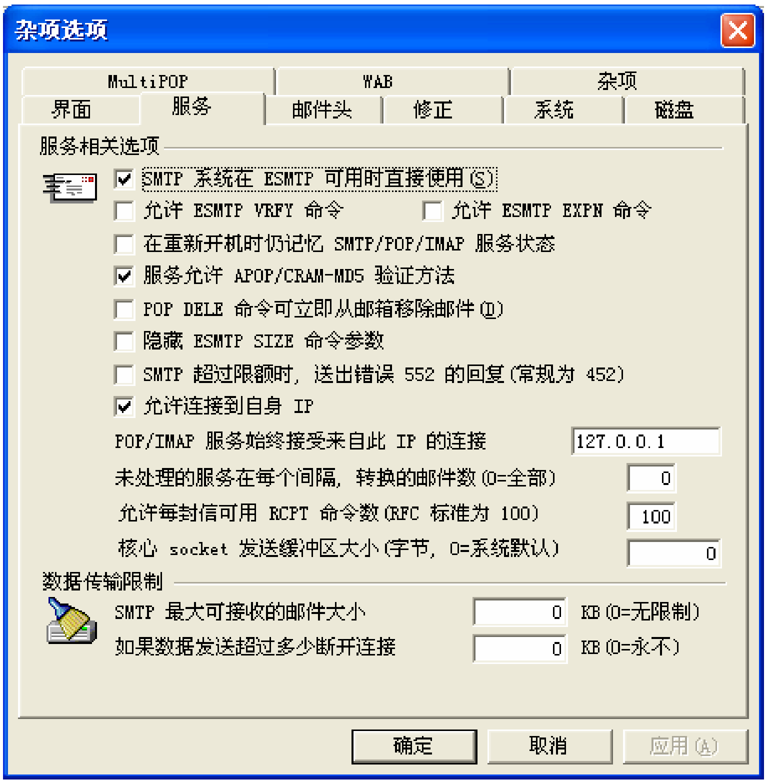
在一个隐藏的窗口中

如果选择此选项，MDaemon 将会创建一个对查看来说，完全隐藏的新的邮件连接窗口。

在一个默认窗口中

如果选择此选项，MDaemon 将会使用将大小与可视化关联的 Windows 所提供的默认设置来创建新的邮件会话窗口。

服务



服务相关选项

<u>SMTP 系统在 ESMTP 可用时直接使用</u>

如果你希望对扩展的 SMTP 命令启用支持，选择此开关。

<u>允许 ESMTP VRFY 命令</u>

点击此开关允许 ESMTP VRFY 命令。

<u>允许 ESMTP EXPN 命令</u>

如果你希望 MDaemon 允许 ESMTP EXPN 命令，点击此选项。

<u>在重新开机时仍记忆 SMTP/POP/IMAP 服务状态</u>

如果启用此控制，MDaemon 将会确保它的服务器（启用或者停用）状态在重启后保持一致。

<u>服务允许 APOP/CRAM-MD5 验证方法</u>

如果你希望 MDaemon 的服务器(POP,IMAP,及其它)允许 APOP 和 CRAM-MD5 认证方法，启用此控制。这些方法通过使得用户利用不发送清楚地文本密码即可被认证成为可能，来提供额外安全。

<u>POP DELE 命令可立即从邮箱移除邮件</u>

点击此开关，MDaemon 将会立即删除用户已经重新找到的邮件，即使 POP 会话并没有合理的完成。

隐藏 ESMTP SIZE 命令参数
如果你希望隐藏 ESMTP SIZE 命令参数，点击此复选框。

SMTP 超过限额时，送出错误 552 的回复（通常为 452）
当尝试递送给超过其配额的收件人，启用此选项将会得到 552 回复（"请求的邮件动作中断：超过存储额度"）。通常为 452 回复（"请求的动作未被操作：系统存储不足"）。

POP/IMAP 服务始终接受来自此 IP 的连接[IP 地址]
POP 和 IMAP 服务器将总是接受来自在此区域输入的 IP 地址的连接，无论如何设置屏蔽和防护设置。

未处理的服务在每个间隔转换的邮件数（0=全部）
如果你希望限制在任何给定的邮件处理间隔被转换的 RAW 邮件的数量，使用此控制。如果达到了限制，MDaemon 将会等待直到在转换更多的邮件前的下一个处理间隔。

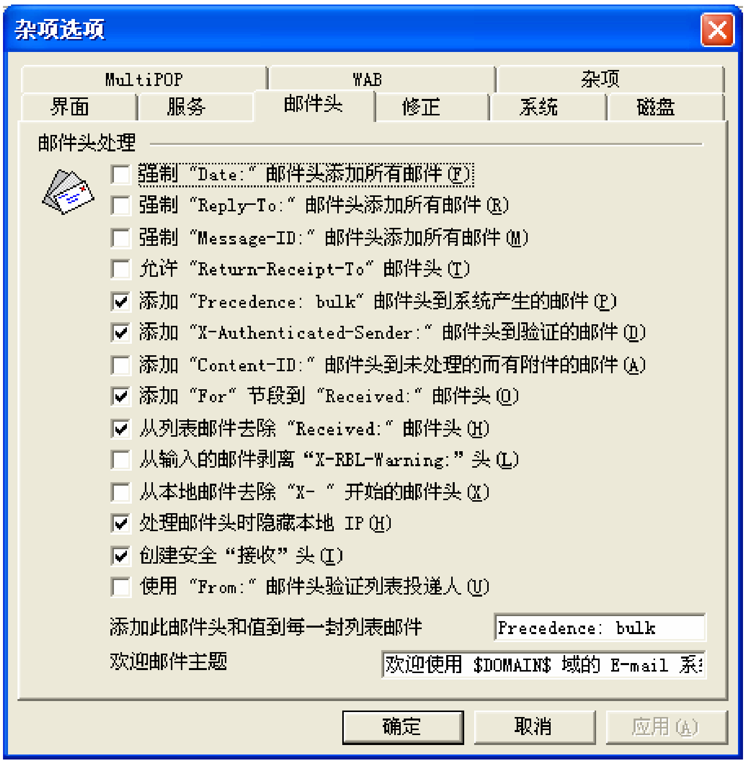
允许每封信可用 RCPT 命令数（RFC 标准为 100）
如果你希望限制每封信可以被发送的 RCPT 命令数量，使用此控制。

核心 socket 发送缓冲区大小（字节，0=系统默认）
如果你希望制定一个非系统默认 socket 发送缓冲区大小，则你可以使用此控制来这么做。在提供的空白处指定新的大小（字节为单位）。

数据传输限制
SMTP 最大可接受的邮件大小
在此设置一个值将会阻止 MDaemon 接受或者处理 SMTP 递送超过某一大小的邮件。当此功能激活时，MDaemon 将会尝试使用在 RFC-1870 种指定的 ESMTP SIZE 命令。如果发送机构支持此 SMTP 扩展，则 MDaemon 将会决定邮件的大小和它的实际的递送并将立即拒绝邮件。如果发送机构不支持此 SMTP 扩展，则 MDaemon 将不得不开始接受邮件，在传送期间，将周期性的跟踪它的大小，并且一旦传输完成，最终将拒绝递送邮件。

如果数据超过多少断开连接 xxKB
如果数据传输在 MDaemon 连接时超过它的极限，MDaemon 将会关闭此连接。

邮件头



邮件头处理

<u>强制在所有邮件中添加“Date：”邮件头</u>

当遇到一封没有“Date:”邮件头的邮件时，如果启用此选项，MDaemon 将会创建一个并且添加到邮件文件中。它将是 MDaemon 首次收到邮件的日期，不是当被发件人创建它时的日期。有几个邮件客户端不能创建此邮件头，这是由于一些邮件服务器拒绝允许此类邮件，此功能将会使它们被发送。

<u>强制在所有邮件中添加“Reply-To：”邮件头</u>

当此选项启用，并且遇到一封没有“Reply-To”邮件头时，MDaemon 将会创建并添加一个在“From”邮件头中发现的地址的邮件文件。如果显示“Reply-To”邮件头但是为空，MDaemon 将会创建类似于此的邮件头：Reply-To：“ ”。这可以修复许多邮件客户端的问题。

<u>强制在所有邮件添加“Message-ID：”邮件头</u>

当遇到一封没有“Message-ID:”邮件头的邮件时，MDaemon 将会随机创建一个，并将其插入到邮件中。

<u>允许“Return-Receipt-To”邮件头</u>

如果你希望允许对从来信中递送确认和发送确认邮件到发件人的请求，点击此复选框。点击此复选框忽略递送确认请求。

<u>添加“Precedence：bulk”邮件头到系统产生的邮件</u>

如果你希望所有系统生成的邮件（欢迎信息，警告，“不能递送”邮件，以及其

他）都插入“Precedence：bulk”邮件头。

添加“X-Authenticated-Sender”邮件头到验证的邮件

如果你希望 MDaemon 添加一个“X-Authenticated-Sender”邮件头到使用 AUTH 命令到达认证会话的邮件，检查此选项。

添加“Content-ID”邮件头到未处理而有附件的邮件

如果你希望添加唯一的 MIME Content-ID 邮件头到 MDaemon 未处理而有附件的邮件，点击此开关。

添加“For”字段到“Received：”邮件头

如果你希望在邮件“Received:”邮件头添加“For [SMTP Recipient]”字段被，点击此开关。

从列表邮件去除“Received：”邮件头

如果你希望从列表邮件中去除所有存在的“Received:”邮件头，点击此开关。有时，这对邮件列表邮件是有用的。

从接收的邮件剥离“X-RBL-Warning：”邮件头

在过去的版本的 MDaemon 中，在邮件递送过程中，任何插入到其他更早版本的 MDaemon 中的 RBL 邮件头会被自动移除。在大多数配置中，此数据应该会保存。如果你希望 MDaemon 继续在投递链中剥除插入早期版本的 RBL 邮件头，点击此复选框。默认设置中，此功能是不启用的。

从本地邮件中去除“X-”开头的邮件头

MDaemon 使用许多服务指定称作 X-Type 邮件头的，这是为了路由邮件并且执行各种不同 MDaemon 特别的功能。此开关将强迫 MDaemon 在它自己之后进行整理，并且从邮件中移除这些邮件头当他们被移动到本地邮箱中。注意：此选项不会移除 X-RBL-Warning 邮件头。

处理邮件头时隐藏本地 IP

点击此选项阻止 Mdaemon 在其处理邮件时，将本地 IP 地址放置到邮件头中。

创建安全“接收”邮件头

在 IP 地址为本地或者通过认证会话接受邮件的时候，如果你希望从收到的邮件头标记中掩饰 IP 地址，PTR 查找结果以及本地机器名，点击此选项。此选项默认为开启的。

使用“From：”邮件头验证列表投递人

通常，发件人到私人列表是使用在 SMTP 会话期间通过的 MAIL FROM 值来检查的。如果你让你的系统使用邮件的“FROM：”邮件头，则启用此开关。

在每一封列表邮件添加此邮件头和值

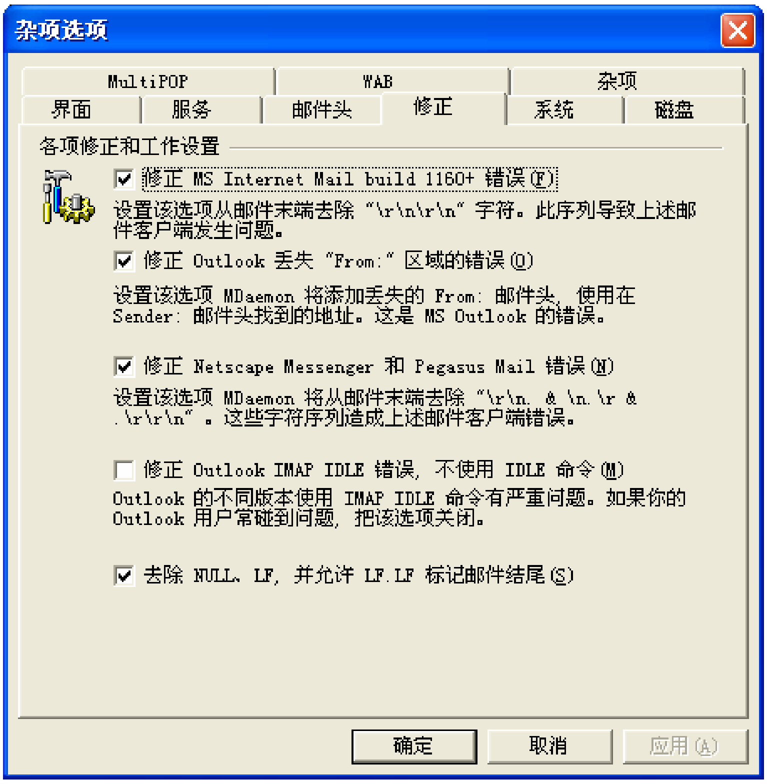
如果你希望添加一个统计邮件头/值组合（比如“Precedence：bulk”）到所有的列

表邮件，则在此指定。

欢迎邮件主题

MDaemon 的特点是发送一封“欢迎”邮件给新帐号。此文本将会作为邮件的“主题”邮件头出现。欢迎信息是由在…/MDaemon/app/目录中包含的 Welcome.dat 文件构成的，并且此主题邮件头可以包含任何在自动回复脚本中包含的宏。

修正



各项修正和工作设置

<u>修正 MS Internet Mail build 1160+错误</u>

此开关已经被添加来尝试处理在邮件被下载后，不显示的 Microsoft Internet Mail 问题。在此开关打开时，MDaemon 将会从邮件主题的末处剥除连贯的 CRLFCRLF 次序。在邮件文件的尾部的 3 组 CRLF 对是 Microsoft 问题的原因。

<u>修正 Outlook 丢失"From:"区域的错误</u>

一些版本的 Microsoft Outlook 在你撰写邮件时，会创建一个 FROM 邮件头失败。FROM 区域信息被替换放置到 SENDER 区域。这将使得下游邮件服务器以及你邮件的收件人混乱。选择此开关，MDaemon 将会使用在 SENDER 区域中找到的地址，创建丢失的 FROM 区域。

<u>修正 Netscape Messenger 和 Pegasus Mail 错误</u>

此开关更正现在不同版本的 Netscape Messenger 和 Pegasus Mail 中的 3 个缺陷的支持。没有此开关的设置，利用那些客户端收集的邮件将会潜在的被它们错误的处理。当检查此选项时，\r\n.,\n.\r 以及.\r\r\n 将会从邮件末尾被去除。

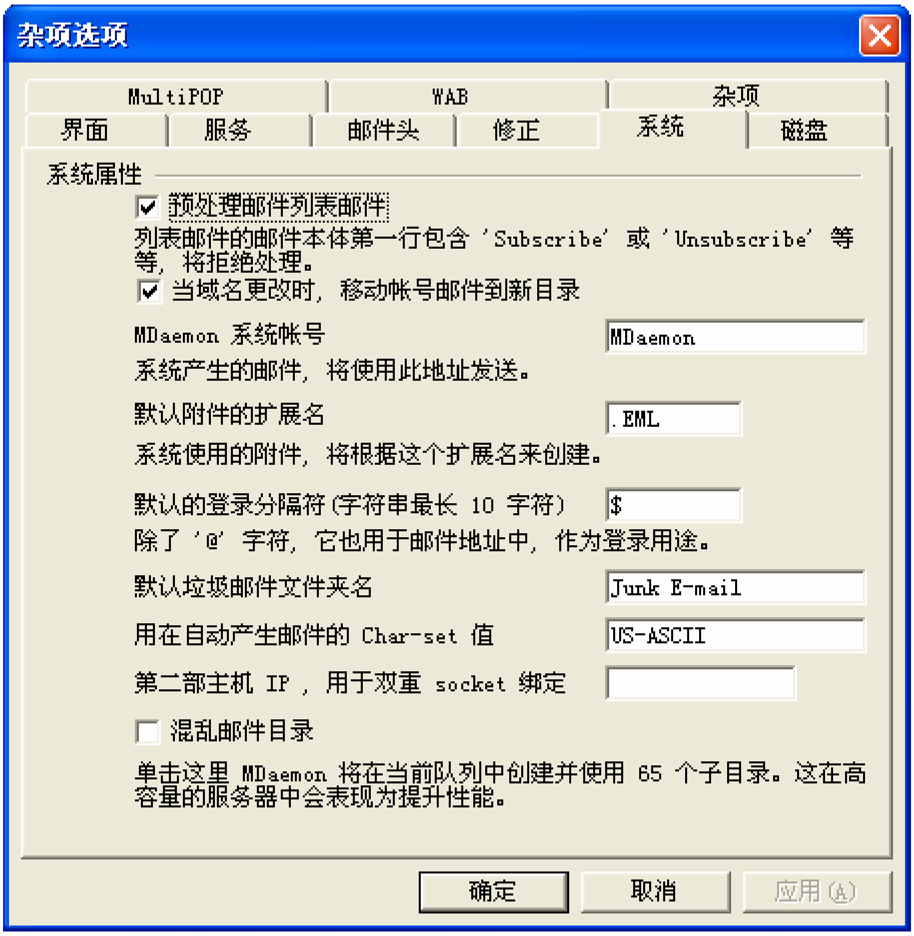
<u>修正 Outlook IMAP IDLE 错误，不使用 IDLE 命令</u>

一些版本的 Microsoft Outlook 对 IMAP IDLE 命令有问题。如果你发现你的 Outlook 用户正在经历这种问题，则点击此复选框关闭对 IMAP IDLE 的支持。

<u>去除 NULL、LF，并允许 LF.LF 标记邮件结尾</u>

对邮件标记末尾允许 Null，EOF 字符以及 LF.LF，以及正常的 CRLF.CRLF 次序。

系统



系统属性

<u>预处理邮件列表邮件</u>

当一封邮件为已经被直接指向系统地址的邮件列表到达时，在此控制启用时，MDaemon 将会拒收它，。例如，一个用户可能通过放置预订或退订命令在 email 邮件的开始，以及发送它到系统地址来加入或者离开一个列表。通常，用户错误的发送这些邮件到它自己的列表。启用此控制将会阻止这些邮件被递送到此列表。

<u>当域名更改时，移动帐号邮件到新目录</u>

如果在你重命名一个域时，此复选框启用，那么那个于已经存在的帐号邮件会必备移送到新名称的目录。否而，MDaemon 将会继续使用就邮件目录名称。

<u>MDaemon 系统帐号别名[地址]</u>

这是系统生成的邮件所来自的地址。预订确认，“不能递送”邮件，各种通知邮件，以及其他的所有系统邮件。

<u>默认附件扩展名</u>

系统生成的邮件将会以此扩展名被创建。这也将系统生成邮件的附件的扩展名。例如，如果 MDaemon 生成一封警告邮件给 postmaster，MDaemon 将创建以“.md”

扩展名的邮件。

*默认登陆分隔符（字符串最大为 **10** 个字符）*

当使用一个 email 地址作为帐号登陆参数时，此字符或者字符串可以被用来作为“@”的另一个选择。这对于一些使用在登陆区域不支持“@”的邮件客户端的用户，可是能非常有用的。例如来说，如果你在此区域使用“$”，则用户可以使用“user@domain.com”或者“user$domain.com”来登陆。

默认的垃圾邮件文件夹名

使用此复选框为 MDaemon 为你的用户自动创建的垃圾邮件文件夹指定默认名。默认名是“Junk E-mail”，与 Microsoft Office 2003 默认匹配。

*用在自动产生邮件的 **Char-set** 值*

指定此字符成为你希望为自动生成邮件使用的设置。默认设置为 US-ASCII。

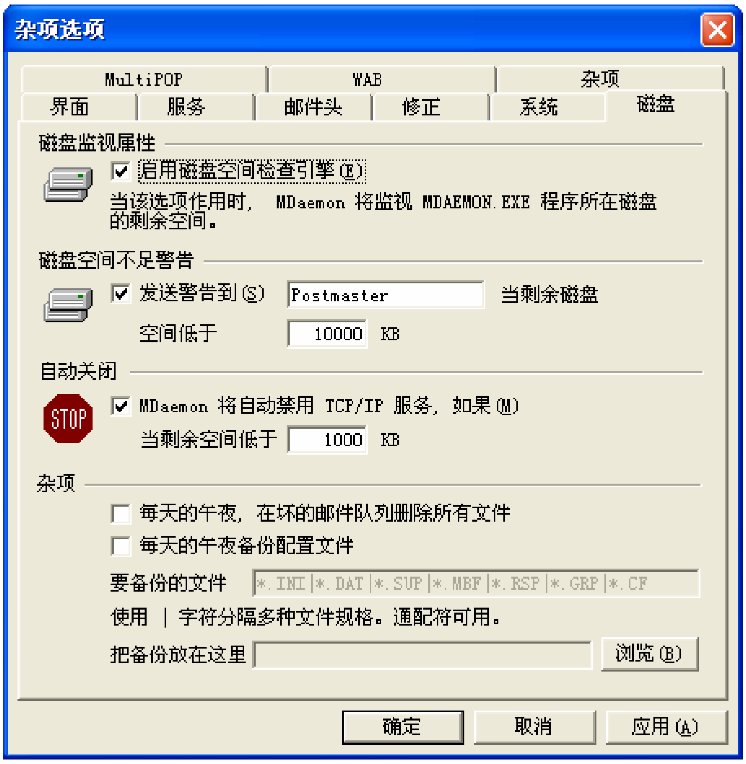
*第二部主机 **IP**，用于双重 **socket** 绑定*

如果你希望主语被绑定到一个附加的 IP 地址，则在此输入。

散列邮件目录

如果你希望启用散列目录，点击此复选框 – MDaemon 将会通过拼凑最多 65 个下级目录来散列某些目录。散列可以为某些高流量站点增加性能，但也可能些微的降低特定 MDaemon 站点。此选项默认为关。

磁盘



磁盘监视属性

启用磁盘空间检查引擎

如果你希望 MDaemon 监视 MDAEMON.EXE 所在的磁盘空间的大小，激活此复选框。

磁盘空间不足警告

发送警告到[用户或者地址] 当剩余磁盘空间低于[xx]KB

通过使用此选项，在磁盘空间下降到某一个级别值时，你可以配置 MDaemon 发送一封通知邮件给你选择用户或者地址。

自动关闭

MDaemon 将自动禁用 TCP/IP 服务，如果当剩余空间低于[xx]KB

在磁盘空间下降到某一个级别值时，如果你希望 MDaemon 关闭 TCP/IP 服务，启用此功能。

杂项

每天午夜，在坏的邮件队列删除所有文件

如果你希望每天午夜，MDaemon 在坏的邮件队列中删除所有邮件，点击此复选框。这可以帮助保存磁盘空间。

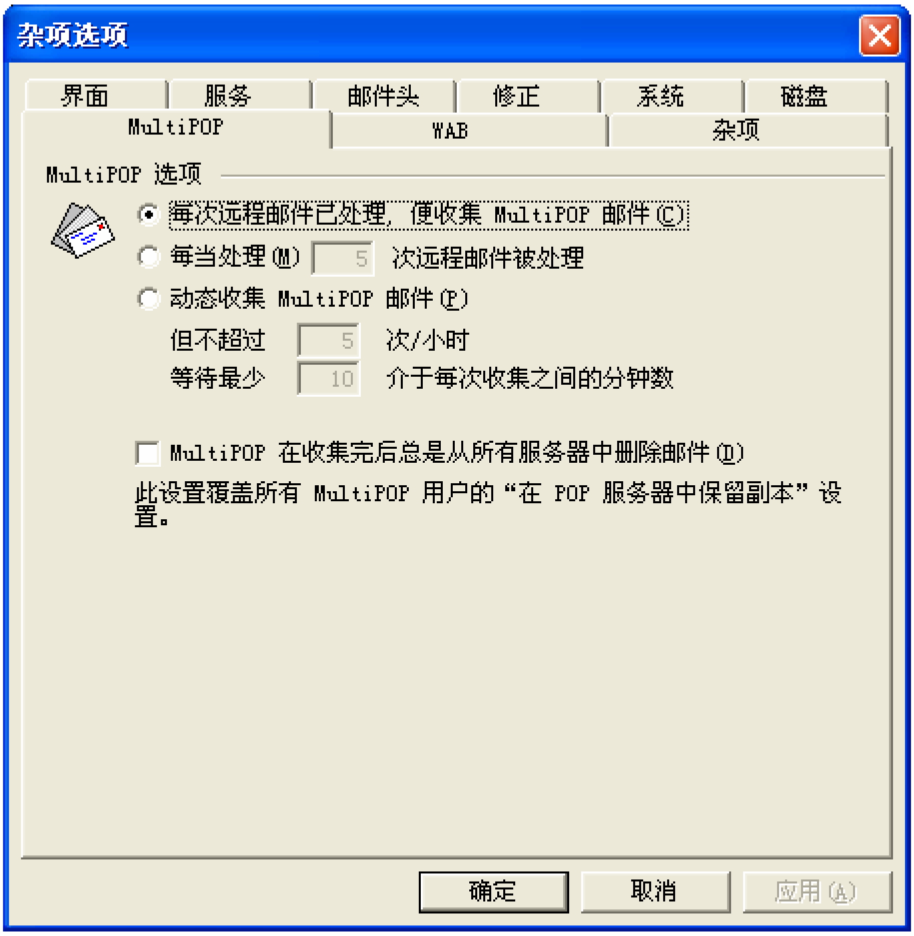
每天午夜备份配置文件

如果你希望每天午夜，存档所有 MDaemon 配置文件，点击此复选框。

要备份的文件
使用此检查框指定额外要备份的文件和文件扩展名。可以使用通配符，并且每一个文件或者扩展名必须使用“|”字符分隔。

把备份放在这里
使用此选项指定你希望存贮备份文件的文件夹

MultiPOP



MultiPOP 选项

每次远程邮件已处理，便收集 MultiPOP 邮件

如果你希望处理每次远程邮件时，MDaemon 收集所有 MultiPOP 邮件，点击此选项。

每当处理 xx 次远程邮件后收集邮件

如果你希望收集 MultiPOP 邮件比处理远程邮件次数少，点击此选项，并在此框中指定一个数字。此数字表示远程邮件在收集 MultiPOP 邮件前处理远程邮件的次数。

动态收集 MultiPOP 邮件

如果你希望动态收集 MultiPOP，点击此选项。通常，每一个远程邮件处理间隔期间，在同一时间为所有用户收集 MultiPOP，或者每 x 数量的间隔。当动态收集时，在每一个用户通过 POP，IMAP 或者 WorldClient 检查他或她的邮件，而不是一次对所有用户时，将为每一个个人用户收集 MultiPOP 邮件。然而，由于 MultiPOP 收集时通过用户检查他的邮件被触发的，那么任何新的 MultiPOP 邮件收集对那个用户来说将是不可见的，直到用户再次检查他的邮件。因为，他将需要检查他的邮件两次，这是为了可以看到新的 MultiPOP 邮件 – 一次触发 MultiPOP，而第二次看到收集到的邮件。

但不超过xx 次/小时

为了减少加载，可以将此 MultiPOP 扩展使用放置到你的 MDaemon 上，你可以使用此控制指定最大数量的为每一个用户收集 MultiPOP 的次/小时。

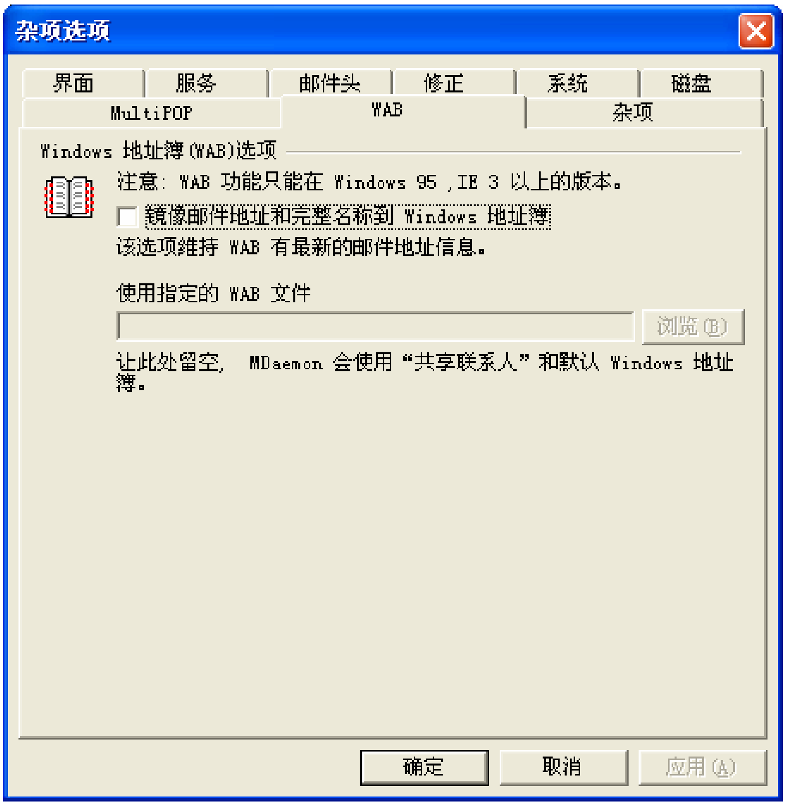
在每次收集之间最少等待xx 的分钟数

此选项可以通过限制用户收集 MultiPOP 的频路，来帮助减少在邮件服务器上的加载。它将限制每用户一次 MultiPOP 邮件收集的时间。指定你希望要求用户在被允许再次检查 MultiPOP 之前等待的分钟数。

MultiPOP 在收集完后总是从服务器中删除所有邮件

如果你希望对所有用户拒绝*在 POP 服务保留邮件副本*选项（在帐号编辑器的 MultiPOP 标签上），点击此选项。所有邮件在收集后将从每一个 MultiPOP 服务器上被删除。

WAB



MDaemon v8 拥有自动保留当前帐号的全名和 email 地址的一个 Windows 地址薄文件（*.wab）或者 Microsoft Outlook 联系人存储。对那些希望在类似于 Outlook 产品用户之间共享地址薄的，当并不希望为此使用 LDAP 服务器或者 ComAgent 的人来说，这是非常有效的

Windows 地址薄（WAB）选项

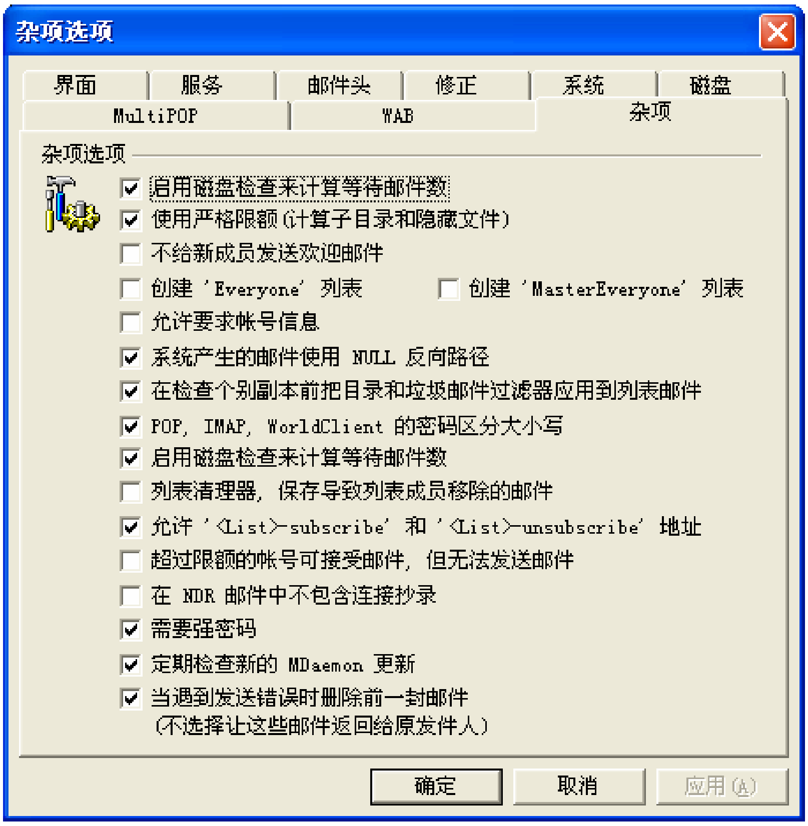
镜像邮件地址和完整名称到 Windows 地址薄

如果你希望你的用户的名称和地址薄被镜像到一个*.wab 文件或者 Microsoft Outlook 联系人存储，启用此检查框。在 Windows 地址薄中，在工具 – 选项菜单，你可以配置是否你的 WAB 通过在 Microsoft Outlook 联系人存储或者一个地址薄（*.wab）文件中存储数据，在 Outlook 和其他应用程序间，将共享联系人信息。

使用指定的 WAB 文件

指定你希望用来镜像你的用户信息的*.wab 文件路径。如果你留此控制为空，则 MDaemon 将会使用在默认 Windows 地址薄中的共享联系人存储。

杂项



启用磁盘检查等待邮件数

此开关控制是否 MDaemon 将检查邮件队列中的等待邮件磁盘。这样做可以使得磁盘长时间运转。

使用严格限额（计算子目录和隐藏文件）

当此框被选，所有文件和下级目录将会受用户的帐号邮箱上大小或者邮件数量限制。否则，只有真实的邮件文件才会计入这种限制。

不给新成员发送欢迎邮件

通过默认值，MDaemon 将会基于 welcome.dat 文件生成一封欢迎邮件，并在创建新用户时，将邮件派送给新用户。如果你想阻止生成邮件，启用此控制。

创建 'Everyone' 列表

如果你不希望'Everyone'邮件列表被你的域创建并维护，清空此框。维护在 MDaemon 域上的每一个用户的邮件列表可能会导致潜在的资源浪费，如果此列表从未被使用过，或者是被很大数量的用户使用的。如果你不希望 MDaemon 创建这些列表，清空此复选框。

允许要求账号信息

当通过 EXPN 或者 LIST 命令要求时，提供用户列表。

系统产生的邮件使用 NULL 反向路径

如果你希望自动生成 email，以一个 NULL 反向路径开发送，点击此复选框。默认值，此开关是开启的，这是为了遵守 SMTPemail 标准，但不管这些标准，一些服务器拒绝接受利用 NULL 反向路径生成的 email，因此你可以清空此选项，如果你愿意的话。但是，在某些情况中（比如自动回复）使用任何其他非 NULL 倒转路径可能导致邮件循环。

在分发单独的邮件列表邮件前，应用内容过滤器规则
当选择了在邮件列表编辑器的路由标签上的 *MDaemon 将检查邮件列表选项*时，启用此控制将会使得在他们被检查并且分发到列表成员前应用内容过滤器规则。

POP，IMAP，WorldClient 的密码区分大小写
在此控制启用时，POP，IMAP，以及 Worldclient 将会区分大小写。

列表清理器删除不包含可解析地址的邮件
当你配置 MDaemon 扫描对于邮件列表的回信，尝试删除不能到达的列表成员，此控制将会使得那些不包括可解析地址的邮件被删除。更多信息，参看邮件列表编辑器的成员标签上的*自动从列表成员中移除废弃的地址*控制。

列表清理器，保存导致列表成员移除的邮件
当 MDaemon 扫描返回的列表邮件，并尝试移除不能被到达的成员地址，此控制将会使得移除列表成员的邮件将被保存。

*允许‘**<List> - subscribe**’和‘**<List> - unsubscribe**’地址*
如果你希望 MDaemon 识别此格式的 email 邮件地址作为合法的（就像实际存在的列表），以便对用户使用简便的方法加入或者离开你的邮件列表。例如，假设你有一个叫做 Mylist@altn.com 的列表。人们将能够通过发送一封 email 邮件给 MyList-Subscribe@altn.com 以及 Mylist-Unsubscribe@altn.com，来预订或者退订你的列表。主题和邮件主体的内容是不相关的。而且，当此功能激活时，MDaemon 将会插入以下邮件头到所有列表邮件：

List-Unsubscribe：<mailto:<List>-Unsubscribe@domain.com>

一些邮件客户端可以识别它，并且自动生成一个对用户可用的退订按钮

超过限额的帐号可接受邮件，但无法发送邮件
正常的，当一个帐号在其上有邮件配额限制时，一旦达到配额，帐号持有者将再不能接受任何以后的邮件。MDaemon 再不能为此帐号接受更多的邮件，直到他或她删除一些超配额帐号中的邮件。但是用户仍可以使用超配额帐号发送邮件。你希望以精确对立的方式 – 当帐号超过限额，它可以仍旧接受邮件但不能发送 – 执行此限制的话，点击此选项。

*在 **NDR** 邮件中不包含连接脚本*
如果你不希望在递送错误和警告邮件中包含 SMTP 会话脚本，点击此选项。

需要强密码
通过默认，当创建新帐号或者更改已存在的密码时，MDaemon 现在需要更强且

跟安全的密码。如果你希望关闭这个强密码限制，清空此复选框。

强且安全密码：

- 必须至少为指定字符长度（默认为 6）
- 必须包含字母和数字
- 必须包含大小写字母
- 可以不包括帐号邮箱或者全名数据。

你可以通过编辑在 MDaemon.ini 中的以下键值，指定最小密码长度：

[Special]

MinPasswordLength=XX (default 6)

*定期检查新的 **MDaemon** 更新*

当启用时，此选项将会使 MDaemon 周期性检查是否有一个对软件可用的更新。当新版本可用时，MDaemon 将提示你，以致你能选择是否下载并安装它。

当删除发送错误的转发邮件

此选项使得遇到递送错误的转发邮件被删除。如果你清空此选项，则那些邮件将被会被返回到原始发件人。

第二部分

MDaemon ® 中文版

MDaemon的帐号功能

第十九章

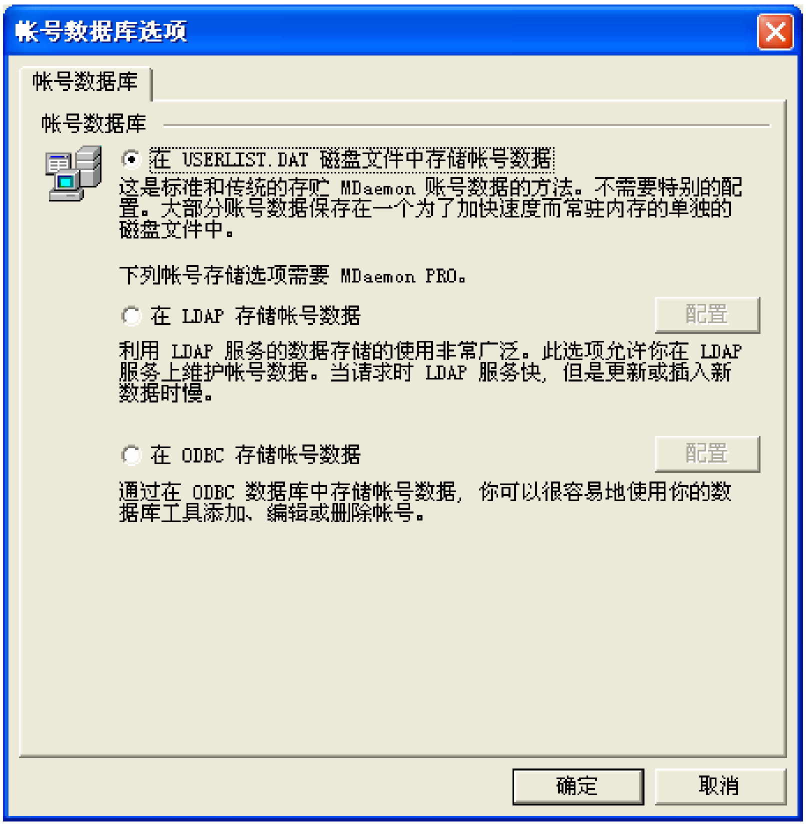
MDaemon ® 中文版

管理MDaemon帐号

管理和编辑你的MDaemon用户帐号

此部分包括在 MDaemon 的帐号数据库选项上的信息，帐号管理器，新帐号默认。帐号数据库选项对话框（Ctrl+M 或者帐号 – 帐号数据库…）用于指定你希望 MDaemon 用来维护你的用户帐号的方法：ODBC，LDAP，或者本地 USERLIST.DAT 系统。帐号管理器（Alt+M 或者帐号 – 帐号管理…）用来维护，创建并删除你的用户帐号。新帐号默认对话框（Alt+F10 或者帐号 – 新建帐号默认值…）是用来指定将被用于新创建帐号的默认设置。

帐号数据库选项



在 USERLIST.DAT 磁盘文件中存储帐号数据

如果你希望 MDaemon 使用它内部的 USERLIST.DAT 文件作为帐号数据库，选择此选项。这是 MDaemon 的默认设置，并且使得所有 MDaemon 用户的帐号信息被存储在本地。更多信息被存储一个单独的文件中，它驻留在内存中以增加效率和速度。

在 LDAP 存储帐号数据

如果你希望 MDaemon 使用你的 LDAP 服务器作为 MDaemon 用户数据库而不是 ODBC 或者它本地的 USERLIST.DAT 系统，选择此选项。如果你有在不同位置你有多个 MDaemon 服务器，但希望他们共享一个独立的用户数据库，你可能希望使用此方法维护你的用户帐号数据。每一个 MDaemon 服务器件将被配置成连接相同的 LDAP 服务器，以便于共享用户信息而不是在本地存储。LDAP 服务器典型的回应迅速，并且对讯问有效率，但是在更新或者插入新数据方面较慢。

配置

当 LDAP 帐号数据选项勾选时，为了配置你的 LDAP 服务器设置，点击此按钮来打开你的 LDAP 选项对话框。

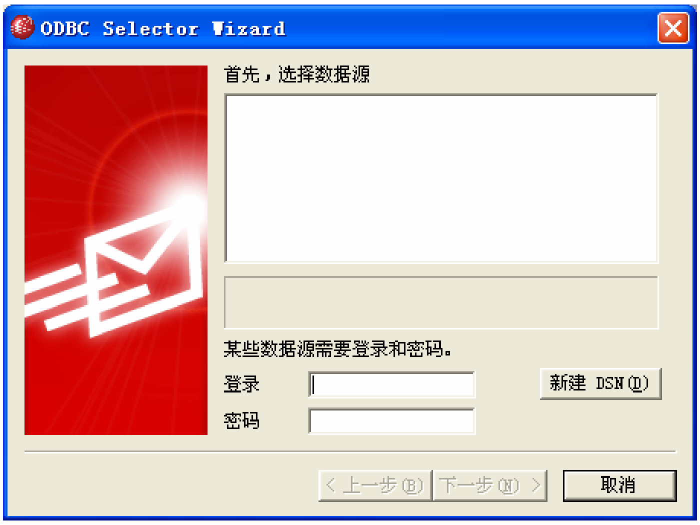
在 LDAP 选项对话框上有个多信息，参看 LDAP 选项。

在 ODBC 存储帐号数据

如果你希望使用 ODBC 适应数据库作为你的 MDaemon 帐号数据库，点击此选项。

配置
当选择了 ODBC 帐号数据选项，点击此按钮打开 ODBC Selector 向导来选择和配置你的 ODBC 适应数据库。更多信息请参看 ODBC Selector。

ODBC Selector向导



使用此向导选择或者配置一个ODBC适应系统数据源来作为你的MDaemon帐号数据库。打开此向导，在 MDaemon 中点击 Ctrl+M 或者帐号 – 帐号数据库…。然后选择所列的选项，"在 ODBC 存储帐号数据。最后，点击在此选项下面的"*配置*" 按钮

首先，选择数据源
此区域列出所有你的 ODBC 系统数据源。选择你希望作为 MDaemon 的用户帐号数据库的之一。
关于启用你的帐号数据库到一个 ODBC 可访问存储的逐步指令，请参看：
转移你的帐号数据库到 ODBC 可访问存储

某些数据源需要登录和密码
如果你选择的数据源需要登录和密码来访问，则在此输入信息。

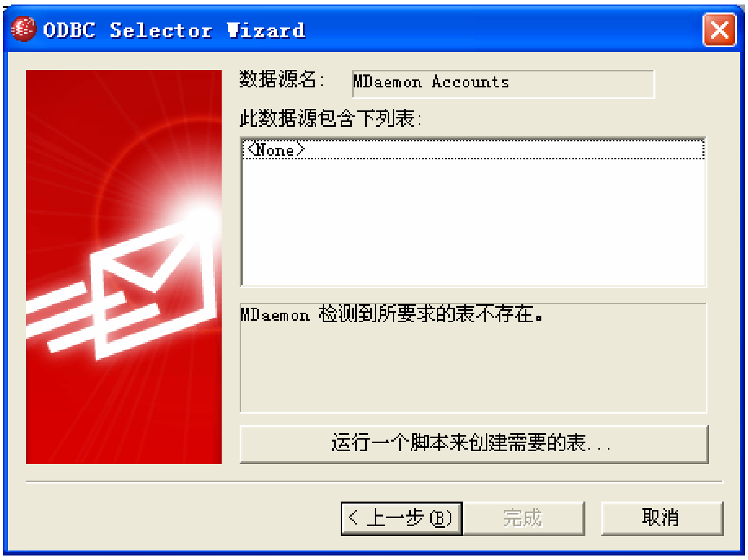
新建 DSN
如果所列的没有一个适应的系统数据源，或者如果你需要创建一个新的，点击新建 DSN。
关于创建新的系统数据源的逐步指令，请参看：
创建新的系统数据源

转移你的帐号数据库到ODBC可访问存储

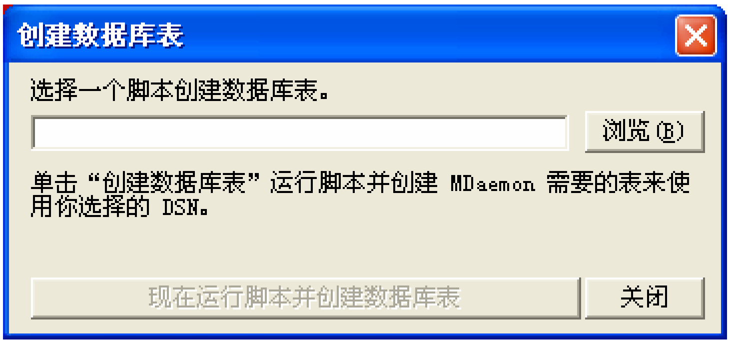
使用 ODBC 可访问数据库作为你的 MDaemon 帐号数据库：
1. 在帐号数据库选项对话框上（帐号 – 帐号数据库…），点击在 **ODBC 存储帐号数据**，然后点击配置打开 ODBC Selector 向导。
2. 选择你希望为你的帐号数据库使用的**数据源**。如果没有列出合适的数据

源，通过依照在创建新的系统数据源下面的所列的指令来创建一个新的。

3. 点击下一步。
4. 如果数据源已经包括 MDaemon 所需要的表格，直接到步骤 7。否则，点击运行一个脚本来创建需要的表



5. 键入文件路径（或者浏览）到你希望为你的数据库应用程序用来创建表格的脚本文件。\MDaemon\app\文件夹包括几个最常用的数据库应用程序的脚本。
6. 点击现在运行脚本并创建数据库表，点击确定，并点击关闭。



7. 点击完成，并点击关闭帐号数据库选项对话框。
8. 数据库转移工具可以转移所有你的用户帐号到 ODBC 数据源，然后关闭 MDaemon。点击确定，然后重新启动 MDaemon 并开始使用新的 ODBC 帐号数据库。

创建新的系统数据源

创建新的 ODBC 系统数据源：

1. 在帐号数据库选项对话框上，点击在 **ODBC 存储帐号数据**，然后点击配置打开 ODBC Selector 向导。
2. 点击新建 DSN 打开选择数据源对话框。打开**机器数据源**标签。

3. 点击**新建…**来打开创建新数据源对话框。
4. 选择**系统数据源**，并点击**下一步**。

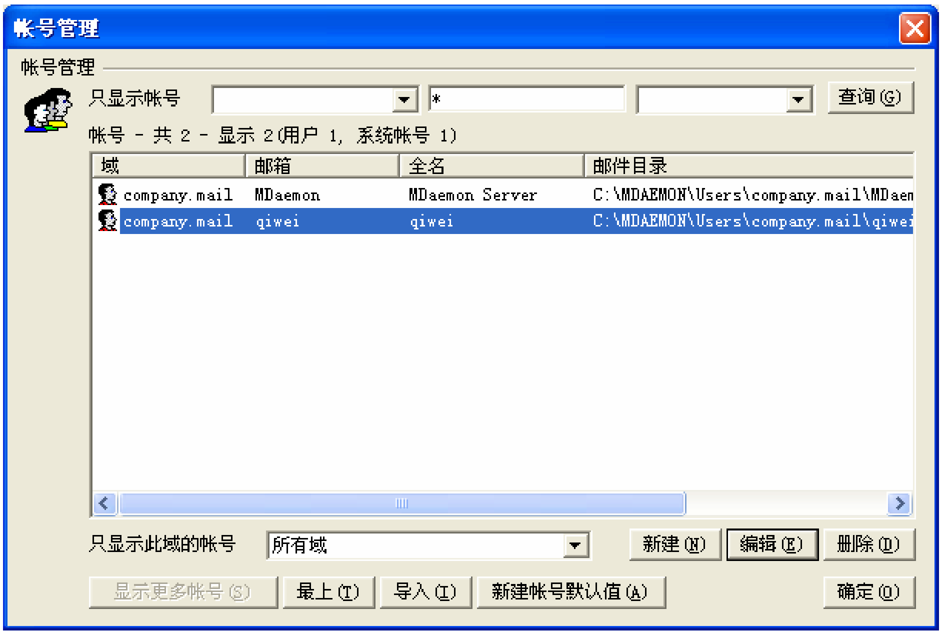
5. 选择你希望设置的数据源的**数据库驱动程序**，并点击**下一步**。

6. 点击**完成**显示指定磁盘设置对话框。对话框的外观基于你将选择的驱动（下面显示 Microsoft 访问设置对话框）。

7. 为你新的数据源指定**数据源名称**，并通过驱动指定对话框提供其他所需（比如创建或者指定数据库，选择一个目录或者服务器，及其它的信息）。
8. 点击**确定**关闭指定驱动对话框。
9. 点击**确定**关闭选择数据源对话框。

帐号管理

为了更好的管理选项，添加，删除，或者你的帐号的调整，MDaemon v8 包括帐号管理（帐号 – 帐号管理…或者 Alt+M）。此对话框提供访问帐号信息以及能够用来通过域，名称或者邮件目录排列帐号。



帐号列表

在帐号列表上，你将可以看到此列表相关的两个统计。第一个数字是当前存在于你的系统上的 MDaemon 用户帐号的总数。第二个数字是那些当前显示在用户列表中的帐号的数量。将会显示的帐号是附随着你在只*显示此域帐号控制*中所选择的。如果你选择了“所有域”，则所有你的 MDaemon 帐号将会显示在列表中。

每一个帐号列表条目列出了它所属于的域，邮箱，帐号的“全名”，以及存储帐号邮件的邮件目录。此列表可以通过你喜欢的栏目，来升序和降序排列。点击任何栏目的标题来以升序排列列表。在此点击栏目，将以降序排列。

注意：
通过默认，一次只有 500 个帐号将被显示在此列表中。如果你希望从当选择的域中看到更多的帐号（或者所有域，如果你已经选择那个选项），则你必须点击“**显示更多帐号**”按钮来显示下 500 个。如果你希望能够一次显示多于 500 个，则打开 MDaemon.ini 文件，更改 MaxAccountManagerEntries=500 键值为你想要的数值。

只显示此域的帐号

从下拉列表框中选择“所有用户”来显示所有 MDaemon 帐号。选择一个指定域将只显示域的帐号。

新建

点击此按钮打开帐号编辑器以便创建一个新的帐号。

编辑

从帐号列表中选择一个帐号，然后点击此按钮在帐号编辑器中打开它

删除
从帐号列表中选择一个帐号，然后点击此按钮删除它。在 MDaemon 将继续处理前，你将被要求确认你删除此帐号的决定。

显示更多帐号
帐号列表一次将只显示 500 帐号。如果在你选择的域中有多于 500 个帐号，则点击此按钮来显示下 500 个。参看上面的注意，其中有如何增加可以被显示的帐号的最大数量的指令。

最上
点击此选项快速移动到帐号列表的顶部。

导入
这将从你可以选择一个导入帐号的文本文件中打开对话框。此按钮与帐号 – 导入 – 从文本文件中…菜单选项中的按钮是一致的。

新建帐号默认值
点击此按钮打开新建帐号默认值对话框。

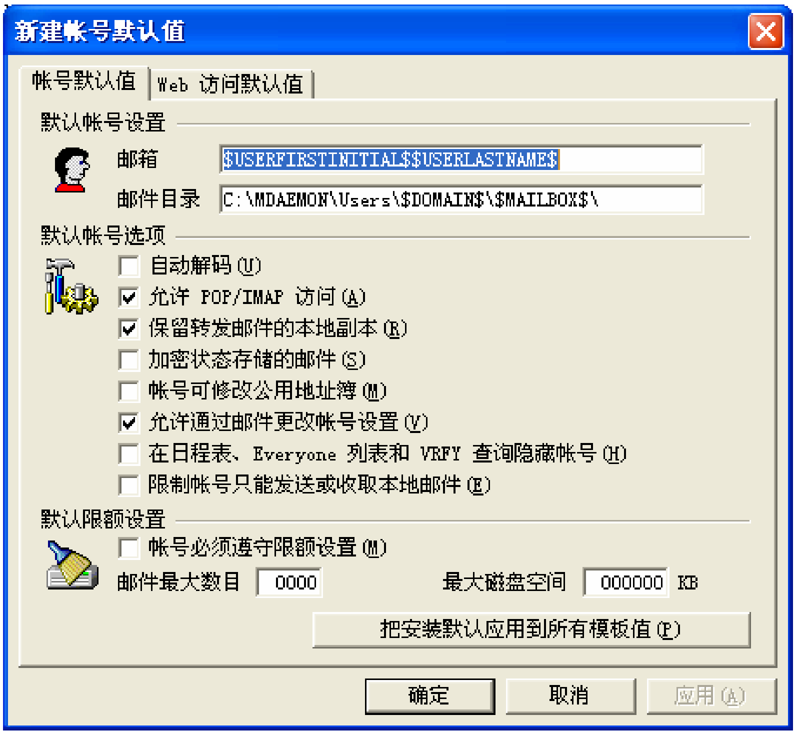
创建MDaemon用户帐号

通过点击在工具栏或者在帐号管理器上的新建帐号按钮，来创建一个新的 MDaemon 用户帐号。这将为配置此帐号打开帐号编辑器。通过使用新帐号默认值对话框，你可以为新帐号制定默认设置。

新建帐号默认值

使用帐号 – 新建帐号默认值…菜单选项来编辑你的帐号默认值以及 Web 访问默认值。

帐号默认值



帐号默认值包括不同的帐号设置控制和模板串。模版是你为普通用户帐号组件制定默认值成为可能。当创建或者倒入帐号时，可以通过使用将被真实值替换的一个不同的特殊宏来构成与帐号相关的不同的串值，比如*邮箱*和*邮件目录*。使用这些模版可以极大地简化和自动化新建帐号管理。

默认帐号设置

邮箱

使用此区域为新建帐号指定默认邮箱名称模版。另外作为邮箱，此值将会是在 USER POP 命令中通过的名称，这将允许从一个远程位置或者 POP 邮件客户端访问邮箱。可以用于模板串中的宏列表，请参看以下*宏*。

邮件目录

使用此区域为新建帐号指定默认邮件目录。实际邮件文件被发送到邮箱的这些目录。必须小心，在此提供的模版必须是一个合法的文件路径。

注意：
MDaemon 支持一个对散列目录的基本系统。在 NTFS 下，例如来说，在同一个根下保持多个目录可能导致性能问题。为了减少此问题，你可以使用新宏$MAILBOXFIRSTCHARSn$，“n”是一个 1 到 10 之间的数字。这将扩展邮箱名称的第“n”字符。更改你的默认邮箱目录模板到类似于以下的值将会存档一个散列目录系统：

```
D:\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS2$\$MAILBOX$\
```

默认帐号选项

此开关用于对各种帐号设置指定默认值。更多此开关信息，参看帐号编辑器。

默认配额设置

此控制用来为新帐号的限额设置指定默认值。更多此控制信息，参看帐号编辑器。

把安装默认应用到所有模板值

点击此按钮将使得在此标签上包含的控制被重置为他们的原始安装默认设置。

模版宏

下面是对自动化你的帐号设置可用宏的快速参考：

$DOMAIN$	此变量将为帐号解决所选的域名称。
$DOMAINIP$	此变量将为帐号解决与当前所选的域相联系的 IP。
$USERNAME$	此变量解决帐号持有者的全名。此区域等同于$USERFIRSTNAME$ $USERLASTNAME$。
$USERFIRSTNAME$	此变量解决帐号持有者的名字。
$USERLASTNAME$	此变量解决帐号持有者的姓氏。
$USERFIRSTINITIAL$	此变量解决帐号持有者的名字的第一个字母。
$USERLASTINITIAL$	此变量解决帐号持有者的姓氏的第一个字母。
$MAILBOX$	此变量解决当前帐号的邮箱名。此指也将作为使用在 POP3 邮件会话中的 POP 用户名使用。这是在 POP 握手会话期间在 USER 命令中的期望值。

Web访问默认值

Web 访问默认值对话框用来指定新帐号将对 WorldClient 以及 WebAdmin 所拥有的默认访问权限。你可以指定帐号是否将能够通过 WorldClient 访问他们的 email，以及是否能够通过 WebAdmin 配置他们的帐号。另外，如果你授予访问 WebAdmin，你可以控制帐号将被允许编辑的设置。

Web 邮件访问默认值

帐号可通过 WorldClient 访问邮件

如果你希望新帐号能够访问 WorldClient 服务器，启用此复选框，这将允许他们通过 Web 浏览器查看他们的 email。

Web 远程配置默认值

帐号可通过 WebAdmin 修改本身的设置

如果你希望授予 MDaemon 用户通过 WebAdmin 修改他们的帐号设置的权限，启用此框。他们只能够编辑那些你在此对话框指定的设置。

当启用此功能，并且 WebAdmin 服务器在邮件路由上设置为活动，用户将能够通过使用他们的浏览器指向 **http://MDaemonsdomain.com:port** 来登入 WebAdmin。他们将首先显示一个登录屏，然后包括他们已经被给予的编辑权限的设置的屏幕。所有他们需要做的是编辑他们选择的任何设置，然后点击*保存更改*按钮。然后他们能关闭他们的浏览器；没有任何登出或者作其他事情的需要。

赋予管理权限的帐号（在个人帐号的 Web 标签上指定）将在登录 WebAdmin 后看到一个不同的屏幕。WebAdmin 内的管理权限的讨论，参看 WebAdmin 用户手册。

默认值，账户可以通过 WebAdmin 做以下操作：

编辑全名

启用此功能将会允许用户调整他们的全名设置。

编辑密码

如果你希望允许用户调整他们的 POP 密码，点击此复选框。

编辑邮件目录位置

此控制用来给定用户调整他们的邮件目录位置的权限。

注意：
你应该在赋予此选项给用户时小心。给用户此权力来更改他们的邮件目录可能让他们访问任何在你的系统上的目录。

编辑转发地址

当启用此功能，用户将能够调整他们的转发地址设置。

编辑高级转发

当启用此功能，用户将能够调整他们的高级转发选项。

编辑加密邮件设置

此功能允许用户控制是否 4096 字节或者更少的邮件信息将被以加密的状态存储到他们的邮箱中。

编辑 IMAP 规则（只有 PRO 版可用）

使用此控制使得用户能够创建和管理他们自己的 IMAP 邮件规则。此功能只有 PRO 版可用。

编辑 EVERYONE 列表设置

此功能允许用户控制是否他们将包括在 MDaemon 的 EVERYONE 邮件列表中。

编辑邮件限制

此检查框控制是否帐号将能够标记他们的“只有本地邮件”设置。

编辑配额设置

如果你希望允许帐号调整他们的配额设置，点击此复选框。

编辑 MultiPOP 设置

如果你希望用户能够启用并关闭 MultiPOP 收集，点击此开关。

注意：
此权限不会以任何方式授予用户创建，删除或者编辑MultiPOP条目的权力。MultiPOP条目必须由管理员使用MDaemon界面创建。此功能允许用户控制是否对他们的帐号的MultiPOP邮件收集是打开的。

编辑自动回复器设置

如果你希望用户能够为他们的帐号添加，编辑或者删除自动回复器。点击此复选框。

编辑允许通过 email 更改

如果你希望允许用户通过特殊 email 邮件调整他们的帐号设置，点击此选项。

立即把这些默认值应用到所有帐号

点击此按钮使得这些默认设置被应用到所有 MDaemon 帐号。任何在个人帐号下已经指定的另外一个选择设置将会丢失;所有当前 MDaemon 用户的 Web 设置将会被更改为在此指定的设置。

第二十章

MDaemon ® 中文版

帐号编辑器

使用MDaemon的帐号编辑器来创建或者编辑帐号

帐号编辑器包括所有MDaemon帐号的设置细节。它用来创建新的用户帐号，以及编辑存在的帐号。当创建一个新的帐号时，在输入用户全名的同时，大部分区域将自动被填充。此自动生成信息是基于模板和在新建帐号默认值中找到的设置。

参看：

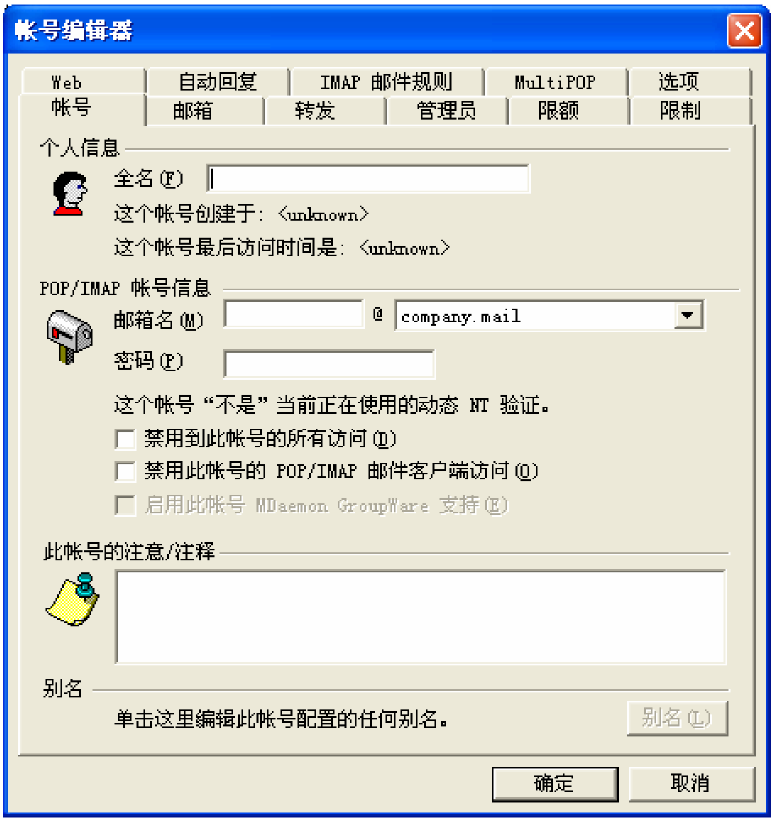
帐号编辑器 – 287 页

新建帐号默认值 – 289 页

创建新的 MDaemon 用户帐号 – 288 页

帐号编辑器

帐号



个人信息

全名

在此输入用户的名和姓。当设置一个新的邮件帐号时，在每一次此区域的值被更改时，都会重新应用模板。全名不能包括“！”或者“|”。

POP/IMAP 帐号信息

邮箱名

此区域为邮箱指定一个唯一的名字，并且也用于作为帐号的 POP/IMAP 登录。另外，邮箱必须是唯一的，且不可包括空格。在输入邮箱的名称后，点击下拉列表框，并选择此帐号的邮箱将会应用到的域。通过默认设置，MDaemon 的主域将会出现在此控制中。邮箱名称不能包括“！”或者“|”。

密码

在此区域输入一个帐号密码。在此区域下，你将看到一个将会告诉你是否动态 NT 人中被用于此帐号的简短陈述。

注意：
你应该总是提供一个密码，即使你不希望允许 POP/IMAP 访问邮件帐号。另外邮件会话验证，用户和密码值被用来允许远程帐号处理和远程文件修补。如果你不希望接受所有的访问，则使用*禁止此帐号的所有访问*选项。

禁用到此帐号的所有访问

如果你希望禁止此帐号的所有访问，点击此选项。用户将不能通过任何方法访问此帐号，MDaemon 也将不能为其接收邮件。MDaemon 将会好像此帐号不存在一样处理。然而，它将仍计入你的许可证的帐号限制中帐号数量。

*禁用此帐号的 **POP/IMAP** 邮件客户端访问*

如果你不希望用户能够通过 POP 或者 IMAP 访问他或她的帐号，点击此选项。此帐号仍可以通过 WorldClient 以及/或者 WebAdmin 来访问，如果这些选项对此帐号启用的话。

*启用此帐号 **OutlookConnector** 的支持*

如果你希望允许帐号使用 MDaemon Outlook Connector 共享 Microsoft Outlook 文件夹，点击此选项。注意：此选项将只能在安装 Outlook Connector 时可用。

此帐号的注意/注释

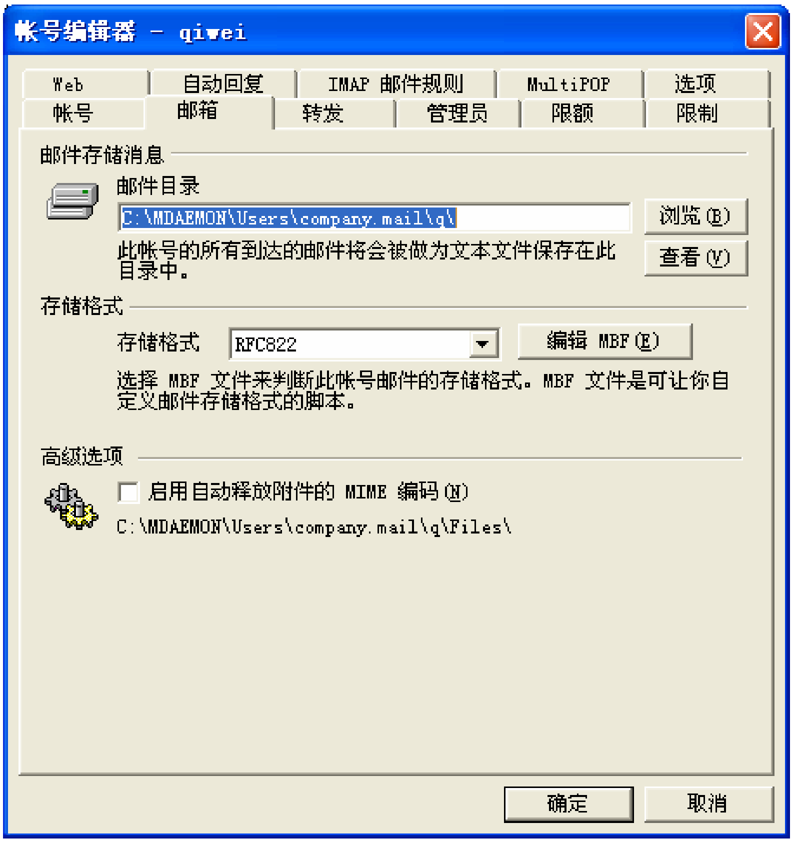
使用此文本区域，来细节化帐号相关的注意和注释。

别名

别名

点击此按钮打开别名编辑器，这将显示当前帐号以及任何指派给所列帐号的别名。你可以使用对话框编辑以前配置的别名或者创建新的。

邮箱



邮件存储信息

邮件目录

输入为该帐号存贮邮件的目录。

存储格式

存储格式

此窗口允许你附属一个 MBF 到邮箱邮件目录。MBF 文件提供一种可能用来与 **MDaemon Server v8** 整合你的已存在的邮件系统的邮件系统兼容性的方法。完整的 MBF 文件讨论以及如何构建他们，参看**创建和使用 MBF** 文件。

编辑 MBF

此按钮允许简单编辑帐号的 MBF 文件。

高级选项

启用自动释放 MIME 编码附件

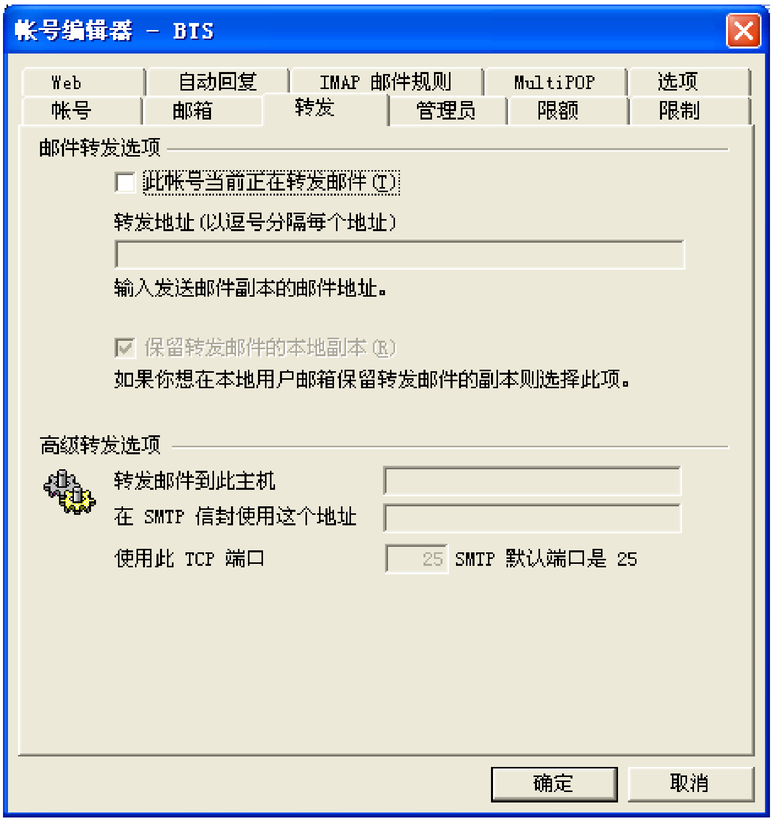
如果设置，此开关使得 **MDaemon Server v8** 自动释放在接收邮件消息中发现的任何 Base64 MIME 深层文件附件。释放的文件将从来信邮件中被移除，解码，并被放置到帐号文件目录中，或者到一些其他的目录，如果你已经设置了附件链接功能并且指定了另外一个的目录。在邮件信息的文字部分将放置一个通知，以代替陈述文件被放置的位置以及文件名的编码数据。如果附件链接启用，那么则一个 html 超链接将会出现在被用来下载文件的邮件中。此功能对于没有

内建 MIME 性能或从需要邮件的文字部分的编码释放到一个单独的文件夹的的邮件传输系统和客户端来说是非常有用的。

通过邮件客户端，比如 Eudora or Microsoft Outlool 或者 Outlook Express，访问他们的帐号的用户可能不希望使用此选项，这是由于这些强大的邮件客户端能够合理的执行 MIME Base64 编码附件。

更多附件链接功能的信息，请参看：附件链接 – 102 页

转发



邮件转发选项

此帐号转发邮件

此开关控制邮件是否将被转发到在*转发地址*区域指定的地址。

转发地址

此区域允许你为此帐号指定一个所有接收邮件的目标地址，一旦邮件到达服务器并且被递送到帐号的本地邮件目录，将会被自动转发到此地址。每一个新到达邮件服务器的邮件将会被自动生成一个副本并被转发到由所选的*此帐号当前正在转发邮件*开关提供的区域指定的地址。

保留转发邮件的本地副本

如果此帐号转发邮件到另一个地址，它可能对 MDaemon 在用户本地邮箱中保留邮件的副本来说是不必要的。此开关控制此动作。

高级转发选项

转发邮件到此主机

如果在此指定邮件主机，则转发邮件将会被递送到此，而不是通过在转发地址区域所指定的值。

在 SMTP 信封使用这个地址

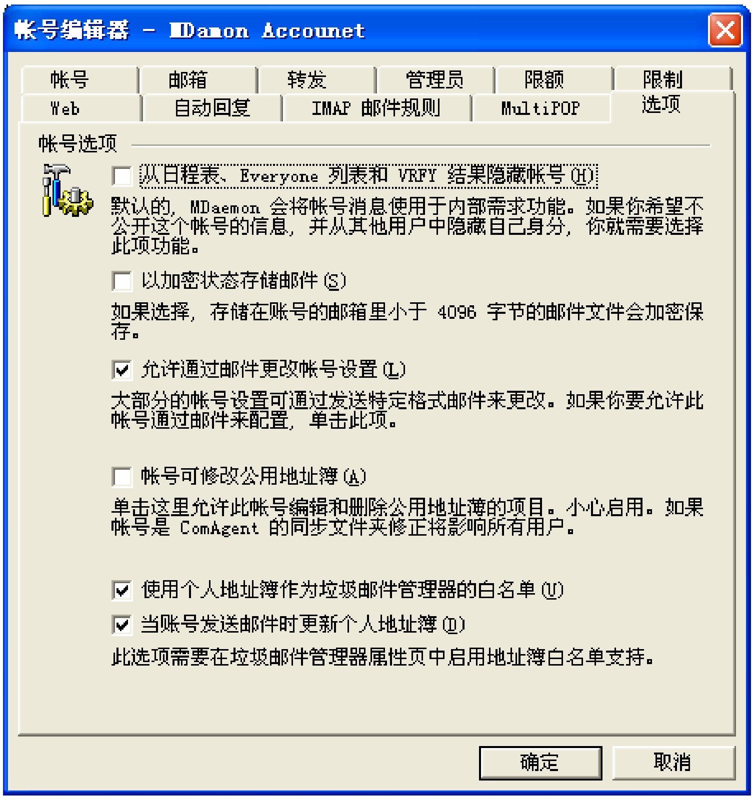
如果在此指定一个地址，此地址将被会用在与接受主机握手会话中使用的 SMTP “Mail From:” 陈述中。通常，邮件的发件人会用在 SMTP 信封的此部分。如果

你需要一个空的 SMTP“Mail From:”命令（就像：MAIL FROM< >），则输入“[trash]”到此控制。

使用此 TCP 端口

MDaemon 将会在此指定的 TCP 端口上发送邮件，而不是默认的 SMTP 外送端口。

选项



帐号选项

<u>从日程表，Everyone 列表和 VRFY 结果隐藏帐号</u>

MDaemon 自动维护一个叫做 MasterEvery@parimary-domain.com 的列表，它可以包含服务器上的每一个帐号。它也可以为每一个叫做 Everyone@users-domain.com 的次域维护列表，次域被包含指定域的所有用户。默认的，当 MDaemon 构成 MasterEveryone 列表时，它将会包括所有域的所有帐号，以及对个人 Everyone 列表和每一个独立域的所有帐号。如果你希望帐号能够私人化并从这些列表上隐藏，点击此复选框。这也将会从日历系统和 VRFY 结果中隐藏帐号。

默认的，用户可以被添加到在“只读”模式中的 MasterEveryone 列表中。如果你希望他们能够被以“正常”模式添加，则更改在 MDaemon 的\app 下级文件夹中的 MDaemon.ini 文件中的以下键值：

MasterEveryoneListReadOnly=No (默认设置为 Yes)

如果你希望完全关闭 Master Everyone 列表功能，则更改以下 MDaemon.ini 设置为以下值：

[Special]

CreateMasterEveryoneList=No (默认设置为 Yes)

<u>以加密状态存储邮件</u>

如果选择，MDaemon 将会为此帐号以加密状态存储邮件。在此状态的邮件将不会是直接可读的，因此提供了一个非常好的保护。当邮件通过 POP 帐号访问时，

MDaemon 将会解密此邮件，但是在存储到磁盘时，此帐号的邮件将会被加密。

允许通过邮件更改帐号设置

此开关决定用户通过远程 email 邮件是否可以访问帐号。此功能允许用户通过发送特殊格式的邮件信息给服务器，来执行普通帐号维护，比如更改密码或者邮件目录。远程帐号操作的更详细讨论，请参看**通过 Email 远程服务器控制**。

帐号可修改公用地址薄

如果你希望帐号能够从 WorldClient 或者 LDAP 公共地址薄中添加和删除条目，点击此选项。

注意：
如果帐号是同 ComAgent 同步文件夹，则调整可能被传播到所有用户。当启用此功能时，请谨慎。

使用默认地址簿作为垃圾邮件过滤器的白名单

垃圾邮件过滤器白名单（自动）包括一个全局设置来使垃圾邮件过滤器忽略那些发件人是在本地地址簿文件中的邮件。使用那个选项，MDaemon 可以对每一封来信查询私人地址薄文件。如果你已经启用了垃圾邮件过滤器选项，但是不希望应用自动白名单到此 MDaemon 用户，则清空此检查框。

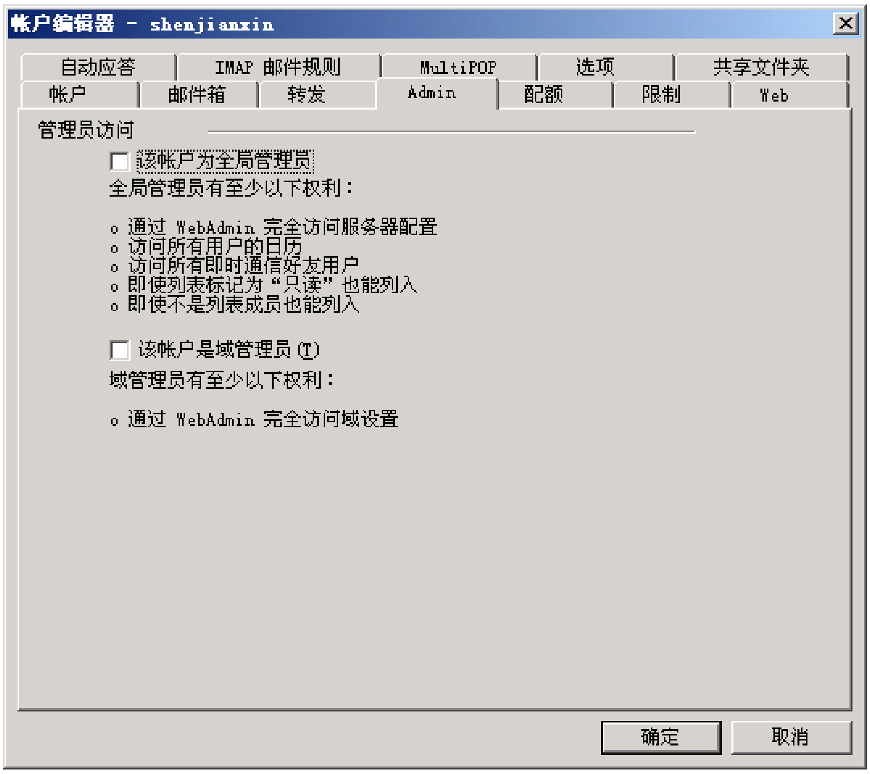
注意：保持你的地址薄与 WorldClient，Outlook，Outlook Express，Windows 地址薄，以及其他使用 Windows 地址薄的 MAPI 邮件客户端更新与同步，可以同过 ComAgent 轻松完成。

当帐号发送邮件时更新个人地址薄

如果你希望在此帐号地址薄添加所有它发送到非本地 email 地址，点击此选项。当提供使用此选项来使用私人地址薄文件作为白名单时，垃圾邮件过滤器错误的数量将明显下降。必须在你使用此功能前启用在垃圾邮件过滤器对话框的白名单（自动）标签上的“启用自动地址薄更新”。

注意：此选项在帐号使用自动回复器时，是关闭的。

管理员



管理员访问

此帐号是全局管理员

开启这个选项来赋予用户服务器级别的管理员访问。服务器级别的管理员访问包括：

对于服务器配置的完全访问，通过 webadmin 对于所有域和所有用户的完全访问。

访问所有用户的日历。

可以作为即时消息的好友来访问所有 Mdaemon 域的所有用户。

即使邮件列表标记为只读，管理员仍然可以给他们发信。

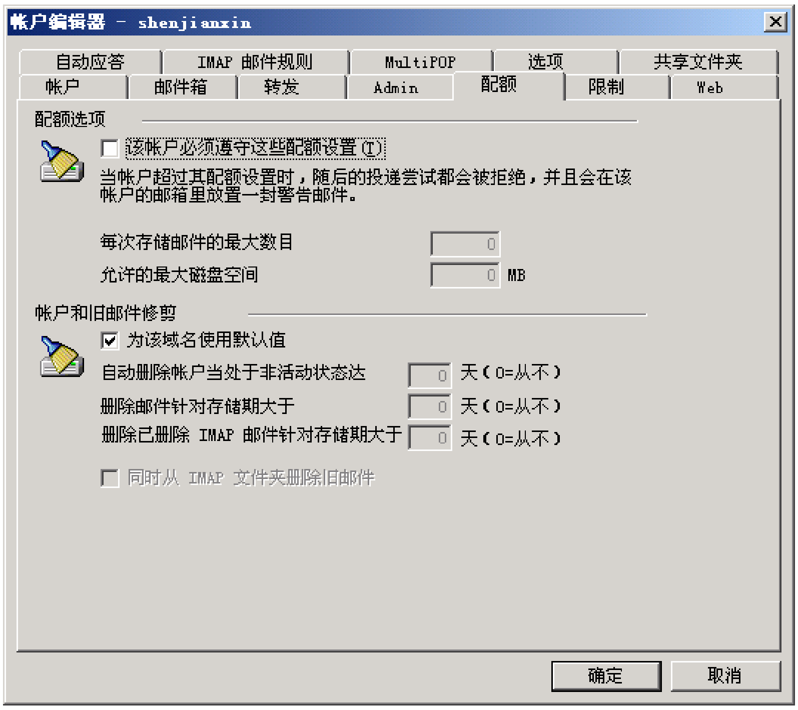
即使管理员不是邮件的成员，然可以给他们发信。

此用户可以对 Mdaemon 所有的文件和选项有完全访问的权限。对于在 webadmin 中管理员的讨论，查看 webadmin 用户手册。

此帐号是域管理员

开启这个选项来指定一个用户为域管理员。和全局管理员类似，只不过他们的管理权限只局限在所在的域。关于域管理员的更多信息，请查看 webadmin 用户手册。

配额



配额选项

<u>此帐号必须遵守这些配额设定</u>

在这里你可以指定该帐号邮箱可以使用的最大邮件数和最大磁盘空间（KB）。如果邮件传递给一个已经超过最大邮件数量限制或最大磁盘空间限制，此邮件将会转发给管理员并发送一个适当的警告信息。如果 MultiPOP 收集将会超过帐号的限制，那么一个类似的警告信息将产生，并且此帐号的 MultiPOP 条目将会自动关闭（但是不会从数据库中移除）。

帐号和就邮件清理

此控制用来指定当帐号不活动时何时被删除。你也可以指定该帐号的旧邮件在一定时间后是否被删除。每天午夜，Mdaemon 将会移除所有超过时间限制的旧邮件，或者彻底删除达到不活动限制的帐号。这些设置的默认值在主域配置（58 页）和次域配置（65 页）上可以指定。如果你想覆盖域的默认值，你可以在此标签上设定。

<u>为该域使用默认值</u>

如果你想为帐号和旧邮件清理使用域的默认值，可以点击这个复选框。这些设置的默认值在主域配置（58 页）和次域配置（65 页）上可以指定。

*<u>自动删除帐号当处于非活动状态大 **XX** 天（**0**=从不）</u>*

在帐号被删除前指定帐号处于非活动状态的天数。0 意味着帐号从不会因为不活动而被删除。

*<u>删除邮件老于 **XX** 天（**0**=从不）</u>*

在邮件被 Mdaemon 自动删除前在帐号里可以保留的天数。0 意味着邮件从不会被自动删除。

删除已标记为已删除 IMAP 邮件老于 XX 天（0=从不）

指定已标记为已删除 IMAP 邮件在用户帐号里可以保留的天数。对于已经标记为删除的 IMAP 邮件在到达指定天数前会被自动清理掉。0 意味着这些邮件被不会因为天数而被自动删除。

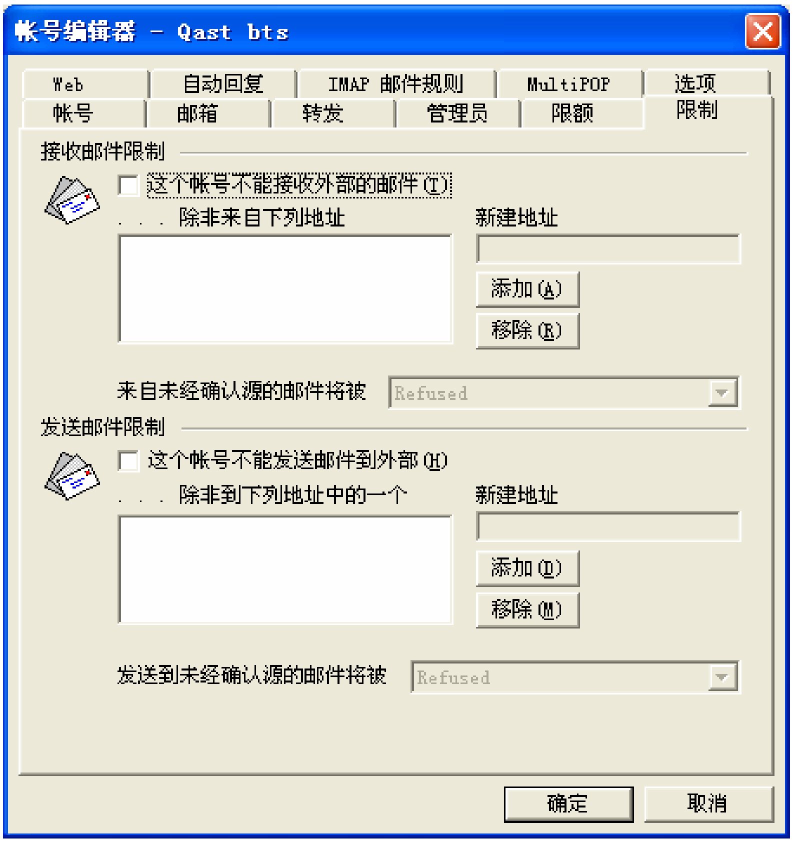
同时也删除 IMAP 文件的旧邮件

如果你想“***删除已标记为已删除 IMAP 邮件…***”也应用到 IMAP 文件夹上。当这个选项被关闭后，在 IMAP 文件夹的邮件将不会被删除。

注意：

当旧的邮件被清理时，而实际上不是真正的删除他们，Mdaemon 将把他们移到“…\badmsgs\[Mailbox]\”文件夹，然后可以管理员被手动删除或晚上的自动进程。这将仅仅作用于旧邮件，--当帐号被清理时候，将连同邮件一起删除掉而不是移动。查看“…Mdaemon\App\”文件夹的 AccountPrune.txt 来获取更多的信息和命令行选项。

限制



使用这个标签上的选项来管理显示的帐号是否可以发送和接收来自或发往非本地域的邮件。在**新建帐号默认值**对话框上有个选项来指定新建帐号是不是默认开启限制选项。

接收邮件限制

这个帐号不能接收外部的邮件

如果你希望显示的帐户不能接收非本地地址邮件，点击此选项。

...除非来自此下列地址

在此区域指定的地址，或作为收信限制的特例。允许通配符。

新地址

如果你希望添加一个地址特例到收信限制列表，则在此输入并点击添加按钮。

添加

在输入一个地址到新地址控制中后，点击此按钮添加到例外列表。

移除

如果你希望从限制列表中删除一个地址，选择地址然后点击此按钮。

来自未认证源的邮件将被...

下拉列表框中的此选项控制 MDaemon 如何处理目标为此邮箱，但来自于非本地或者其他未认证域的邮件。你可以选择以下选项：

拒绝—限制的邮件将被 Mdaemon 拒绝。
返回给发件人—限制的邮件被退回发件人。
发送给管理员—限制的邮件将会被接收但是会被发送给管理员。

外发邮件限制

这个帐号不能发送邮件到外部

如果你希望显示的帐户不能发送非本地域邮件，点击此选项。

…除非到下列地址中的一个

在此区域指定的地址，或作为发信限制的特例。允许通配符。

新建地址

如果你希望添加一个地址特例到发信限制列表，则在此输入并点击添加按钮。

添加

在输入一个地址到新地址控制中后，点击此按钮添加他到例外列表。

移除

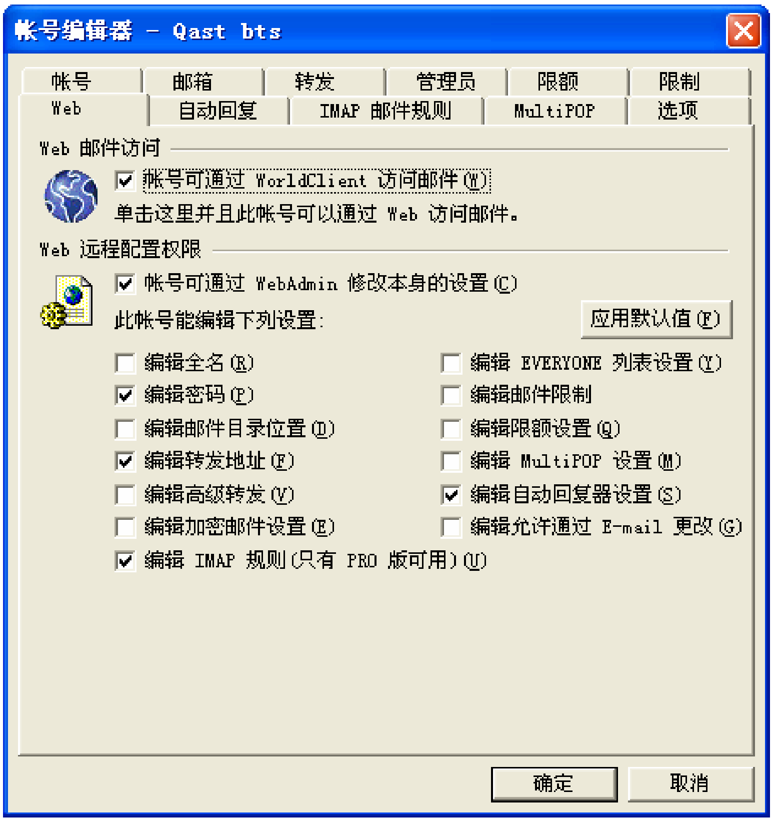
如果你希望从限制列表中删除一个地址，选择地址然后点击此按钮。

发送到未认证源的邮件将被…

下拉列表框中的此选项控制 MDaemon 如何处理来自此帐号，但目标为非本地或者其他未认证域的邮件。你可以选择以下选项：

拒绝—限制的邮件将被 Mdaemon 拒绝。
返回给发件人—限制的邮件被退回发件人。
发送给管理员—限制的邮件将会被接收但是会被发送给管理员。

Web



Web 邮件访问

通过 WorldClient，账户可以访问邮件

如果你希望用户可以访问 WorldClient 服务器，启用此复选框，这个选项可以让他们使用 web 浏览器检查他们的邮件。

Web 远程配置权限

账号可通过 WebAdmin 修改本身的设置

如果你希望授予 MDaemon 用户许可权，通过 WebAdmin 来调整他们的账户设置，启用此功能。他们只能编辑那些你在下面启用的设置。

如果用户被赋予全局或者域管理权限，那么在他们登陆 WebAdmin 后，将看到一个不同的界面。

编辑全名

启用此功能将允许用户调整全名设置。

编辑密码

如果你希望允许用户调整他们的账户密码，点击此复选框。

编辑邮件目录位置

此控制用于赋予用户权限，来调整他们的邮件目录位置。

注意：

> 在赋予用户权限方面，你应该十分谨慎。赋予用户改变他们邮件目录的权利可能使他们访问其他在你的系统中的目录。

编辑转发地址
当此功能启用时，用户将能够调整他们的转发地址设置。

编辑高级转发
当此功能启用时，用户将能够调整他们的高级转发选项。

编辑 IMAP 规则
使用此控制可以使用户创建并管理他们自己的 IMAP 邮件规则。

编辑 EVERYONE 列表设置
此功能允许用户控制 MDaemon 的每个人邮件列表中是否包括他们。

编辑配额设置
如果你希望允许账户调整他们的配额设置，点击此开关。

编辑 MultiPOP 设置
如果你希望允许用户可以启用或停用 MultiPOP，点击此开关。

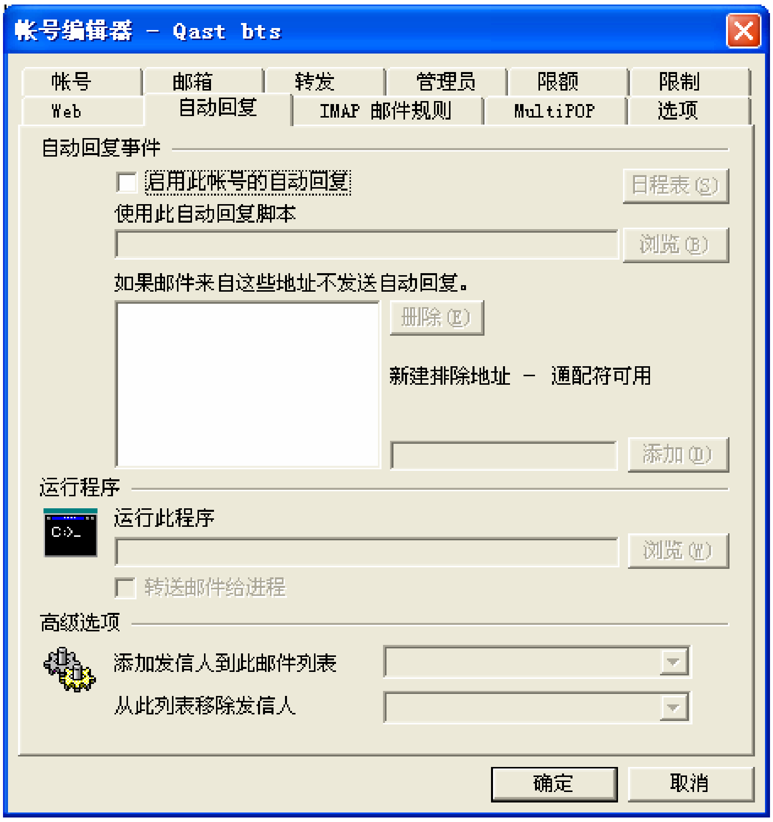
不管怎么样这个设置不会给用户权限去创建，删除，或编辑 MultiPOP 条目。MultiPOP 条目必须由管理员使用 Mdaemon 界面创建。这个功能只是允许用户控制帐号 MultiPOP 收集是否打开。

编辑自动回复设置
如果你希望用户可以添加，编辑，或者删除他们账户的自动回复，点击此复选框。

编辑允许通过 E-mail 更改
如果你希望允许用户通过特殊格式邮件信息，调整他们的账户设置，点击此复选框。

应用默认值
点击此按钮会使得在 Web 访问默认对话框中指定的默认值被应用到 MDaemon 账户。任何在个人账户上指定的更改设置会被 Web 访问默认值所替代。

自动回复



自动回复事件

启用此帐号的自动回复

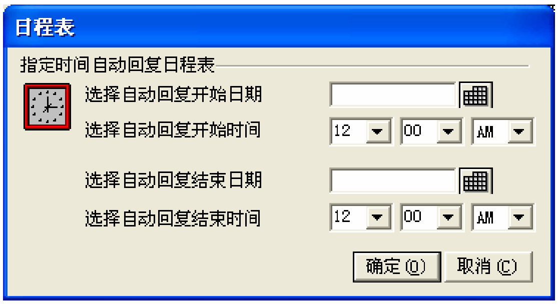
启用此控制会为此账户激活自动回复。

使用此自动回复脚本

此区域指定自动回复文件（*.RSP）的完整路径和文件名。此文件首先将通过与 MBF 文件关联的过滤机制。在 MBF 文件中允许使用的键值将也可在自动回复文件中允许使用。

日程表

点击此按钮打开日程对话框，在这上面你可以设置激活自动回复的开始和结束日期与时间。如果你希望那个自动回复一直活动，留空此框。



如果邮件来自这些地址不要发送自动回复

这里，你可以列出你希望被自动回复地址。

> 注意
> 有时候自动回复邮件发往一个地址，然后又会返回一个他自身的回复。这将会创建一个“ping-pong”效应导致邮件不断在两个服务器之间回复。你可以使用这个功能来阻止 Mdaemon 自动回复那些在这指定的地址。

删除
点击此按钮从例外地址中删除选择的条目。

新建排除地址---通配符可用
如果你希望那个添加一个地址到例外地址列表，在此输入并点击添加按钮。

添加
在新建例外地址文本框中输入一个地址，点击此按钮来添加它到例外地址列表中。

运行程序
运行此程序
此区域给一个程序指定完整路径和文件名，此程序将会在新邮件到达指定邮箱时启动。

高级选项
添加发信人到此邮件列表
如果在此区域输入邮件列表，那么邮件信息的发送者将会被自动添加进邮件列表。对于创建自动列表来说，这是一个非常便利的功能。

从此列表移除发信人
如果在此区域输入邮件列表，那么邮件信息的发送者将会被自动从指定邮件列表中删除。

提示
自动回复事件总是被远程邮件所触发。如果是来自本地用户，那么是否触发自动回复在**杂项对话框**进行设置。这个选项是：*自动回复由本地和远程邮件触发*，开启这个选项，你希望本地邮件也会触发自动回复。

IMAP邮件规则

使用 Mdaemon,IMAP 用户可以使他们的邮件自动分发到服务器上指定的文件夹。和内容过滤器类似，Mdaemon 将检查每个邮件的邮件头然后和规则进行匹配。如果邮件匹配他们的规则，Mdaemon 将把邮件移往在规则里指定的文件夹。这个办法比起在客户端过滤邮件是很有效的。由于一些 IMAP 客户端甚至不支持邮件规则和过滤，IMAP 邮件规则提供这个功能给这些客户端。

IMAP 邮件规则和邮件目录可以通过帐号编辑器上的 IMAP 邮件规则在服务器上直接创建。用户也可以通过特殊格式的邮件来创建。对于 IMAP 邮件规则的支持已经被加入到 webadmin 中。只需要简单的在浏览器中登陆 webadmin，用户可以管理他们自己的帐号规则和设置。通过 webadmin，你可以让用户完全控制自己的规则，从而避免替他们维护这些功能。

现有的 IMAP 邮件规则

这里列出了所有为用户帐号所创建的规则。处理规则的时候是按照罗列的次序来进行，直到找到一个匹配的规则。因此，一旦一个邮件匹配了一个规则，那么邮件将被移动到规则里指定的文件夹，然后对于这个邮件的规则处理也就结束了。使用向上向下按钮来调整规则的位置。

移除

单击列表中的一条规则然后单击*移除*从列表中删除。

全部清除

单击这个按钮将删除用户的所有 IMAP 邮件规则。

向上
单击列表中的一条规则然后单击这个按钮把它移到列表中更高的位置。

向下
单击列表中的一条规则然后单击这个按钮把它移到列表中更低的位置。

新建 **IMAP** 邮件规则
使用此项来为用户创建新的 IMAP 邮件规则。

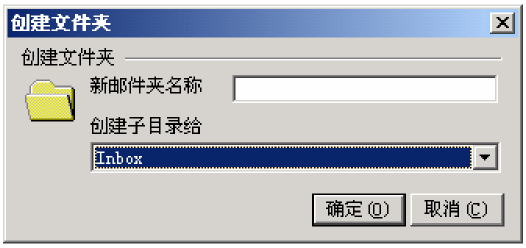
如果[...]邮件头
在此输入一个邮件头或从下拉框中选择。Mdaemon 将会在所有接收的邮件中搜索该邮件头，查找在下面指定的文本信息。然后，根据匹配的情况，将决定哪个邮件应该被移送到规则指定的文件夹。

比较下拉框
这个是邮件头和 IMAP 规则的比较类型。Mdaemon 将会搜索指定的邮件头，查找在下面指定的文本信息，然后根据此控制的设定来处理—邮件头的文本信息完全匹配，不完全匹配，包含文本，一点也不包含，以它为开始，等等。

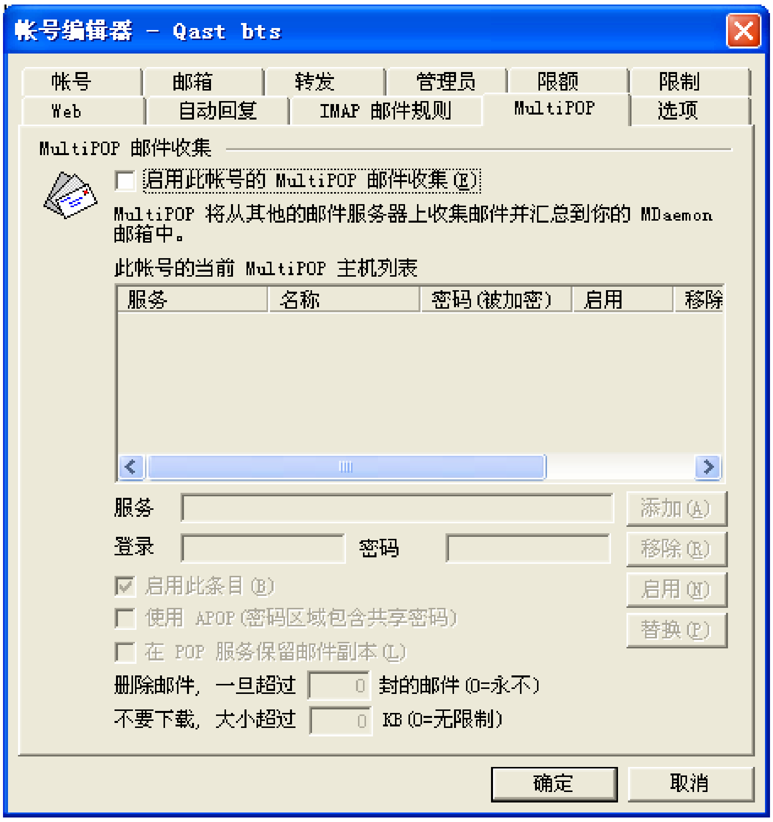
此文本
输入文本作为 IMAP 邮件规则中指定 Mdaemon 搜索邮件头并查找的信息，

然后移动邮件到该文件夹
在为一个规则指定了若干参数后，单击你想要匹配规则的邮件移动到的文件夹。然后单击“添加”按钮来创建。

新建文件夹
单击这个按钮来创建一个新的文件夹。这将打开一个创建文件夹对话框，在此，你可以指定文件夹的名字。如果你希望让它成为一个现有文件夹的子文件夹，那么就从下拉框中指定文件夹。



MultiPOP



MultiPOP 功能允许使用无限数量的 POP 主机/用户/密码混合邮件信息收集。这对那些在多个服务器上拥有邮件帐户，而又希望将邮件收集并保存在一个地方的用户来说，非常有用。在分发到用户邮箱前，MultiPOP 收集邮件首先放置到本地队列中，以使它能像其他拥有自动回复和内容过滤器的邮件一样被处理。

MultiPOP 邮件收集

<u>为该用户启用 MultiPOP 邮件收集</u>

点击此按钮切换所选 MultiPOP 条目的状态。此开关赋予你在 MDaemon 执行它的 MultioPOP 线程时，控制其是否为此条目收集邮件。

<u>服务器</u>

输入你想要收集邮件的 POP3 服务器。如果你希望指定一个端口来收集邮件而不是使用 Mdameon 默认的端口，你可以在主机后面添加一个新的端口号，用冒号隔开。例如，“mial.altn.com”将使用默认的端口来收集邮件，而“mail.altn.com:523”将会连接到 POP3 服务器的 523 端口来收集邮件。

<u>登录名</u>

输入 POP3 用户名或登录名来访问指定服务器的邮件帐号。

<u>密码</u>

输入 POP3 密码或 APOPA 共享密码来访问指定服务器的邮件帐号。

*使用 **APOP**（密码字段包含共享密钥）*

单击这个选项，如果你想使用 APOP 这个认证方法来从指定的服务器收取邮件。注意：当这个选项选中的时候，密码字段必须包含共享密钥。

*在 **POP** 服务器上保留邮件副本*

单击这个复选框，如果你希望在服务器上保留邮件的副本。如果你希望以后在别的地方还要收取邮件，这是非常有用的。

*删除邮件累计[xx]或更多（**0**=从不）*

这是 MultiPOP 保留在远程 POP 服务器上邮件的数量。当你收集邮件的时候，任何一个超过此数量的邮件将被删除，将保留最老的邮件。例如：如果你在此指定“200”，那么最早的 200 封邮件将保留在服务器上。每次 MultiPOP 去收取邮件的时候，这些邮件都将会保留，但是多余的邮件将会被下载下来然后从服务器删除。指定“0”如果你不希望删除任何邮件，而不管存储了多少邮件。

注意：有些 ISP 将会限制邮件的存储的数量，所以你必须和他们确认有关帐号的限制。

*不要下载大于[**XX**]**KB** 的邮件（**0**=不限）*

在此输入一个值来指定该大小的邮件不被下载。

移除

单击这个按钮从列表中移除选定的 MultiPOP 条目。

开启/关闭

点击此按钮切换所选 MultiPOP 条目的状态。此开关赋予你在 MDaemon 执行它的 MultioPOP 线程时，控制其是否为此条目收集邮件。

添加

按此按钮添加你的值到 MultiPOP 纪录列表。

替换

当从此列表选择条目时，它将会显示出来进行编辑。在作出任何希望的更改后，点击此按钮来应用它们。

移除

单击这个按钮从列表中移除选定的 MultiPOP 条目。

共享文件夹

注意：只有当共享文件夹对话框上*开启用户文件夹共享*启用的时候，此标签才可用。

IMAP 文件夹

此区域显示用户所有的 IMAP 文件夹，并可以被用来与其他 MDaemon 用户对他们共享访问。当帐号最初创建时，此区域为空，直到你使用*文件夹名*和*创建*控制（或者在 IAMP 邮件规则标签上的控制）来为其添加一个文件夹。在此列表中的下级文件夹，将使文件夹和下级文件夹名称通过在共享 IAMP 文件夹对话框的共享文件夹标签上指定的分隔符分离。

移除

从列表中移除共享 IMAP 文件夹，选择文件夹，然后点击移除按钮。

新建 **IMAP** 文件夹

文件夹名称

添加新文件夹到此列表，在此控制中为其指定名称并点击创建。如果你希望新文件夹作为此列表中文件夹的一个下级文件夹，则将母目录名称作为新文件夹名称的前缀，并在共享 IMAP 文件夹对话框的共享文件夹标签上指定分隔符。例如，如果分隔符是‘/’，并且母目录是‘My Folder’那么新文件夹的名称应该为‘My Folder/My New Folder’。如果你不希望它作为一个下级文件夹，那么新文件夹名称应为‘My New Folder’，而没有前缀。

新建

在指定文件夹的名称后，点击此按钮添加文件夹到此列表。

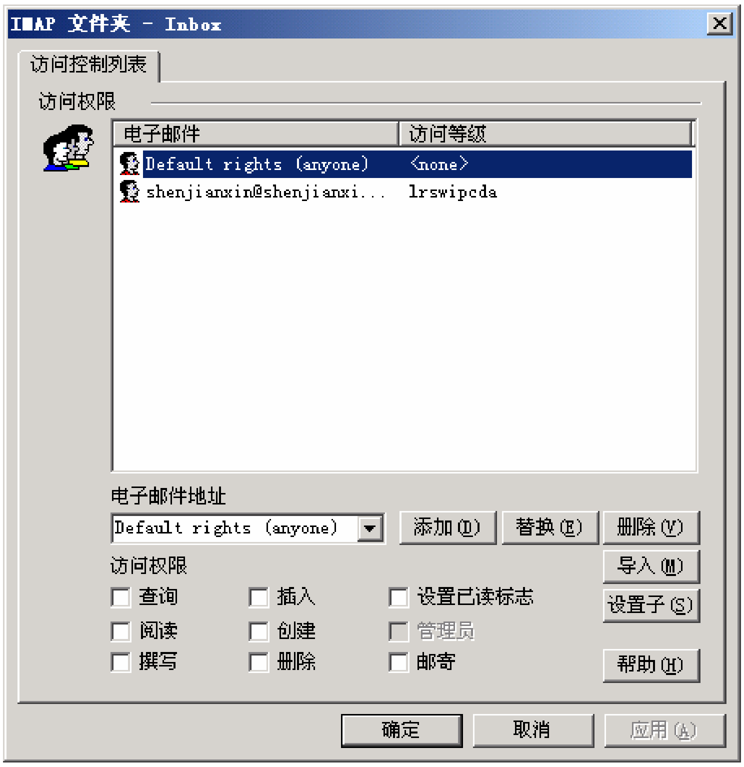
替换

如果你希望编辑共享文件夹之一，点击条目，做出更改，然后点击替换。

编辑访问控制列表

选择一个文件夹，然后为此文件夹，点击此按钮打开访问控制列表对话框。使用访问控制列表对话框指定能够访问文件夹的用户，以及每一个用户的权限。

访问控制列表



访问权限

此区域用来指定你希望授予访问共享文件夹权限的 MDaemon 用户帐户，并为每一个用户设置访问权限。你可以从账户编辑器的共享文件夹标签上到达此对话框。双击指定的目录，或者单击文件夹，然后点击编辑访问控制列表，来打开访问控制对话框。每一个条目列出帐户的 email 地址，并且你可以授予用户每一个访问权的一封信的访问等级。

Email 地址

从下拉列表中，选择你希望授予权限的共享文件夹的 MDaemon 帐户。

添加

在从列表中选择一个 Email 地址后，并且你希望授予用户的访问权利，点击添加，添加帐户到列表。

替换

为了调整一个已存在的访问权限条目，选择条目，做出任何对访问权限渴望的更改，然后点击替换。

移除

从访问权限列表移除一个条目，选择渴望的条目，然后点击移除。

导入

利用导入功能，你可以添加一个已存在邮件列表的成员到具有访问权限的用户列表。选择你希望授予给用户的访问权限，点击导入，然后双击渴望的列表。所有列表成员将会被添加到带有你设置的权限的列表。

帮助

点击帮助显示访问权限列表和他们的定义。

第二十一章

MDaemon ® 中文版

导入帐号

导入帐号到MDaemon

MDaemon 服务器 v8 支持多种导入用户帐户的方法。他们可以从 NT SAM 数据库中，SLMail 用户数据库导入，或者直接从文本文件中。MDaemon 的导入功能可以从帐户 – 导入…菜单选项中到达。

从文本文件中导入帐号

点击帐号 – 导入… →从标点分割的文本文件中导入帐号…菜单选项，访问此帐号产生功能。从*帐号管理器*上的*导入*按扭也可以访问此功能。这是一个导入帐号和产生邮件帐号的简单方法。Mdaemon 会读取一个文本文件然后产生一个新的包含姓名的邮件帐号。如果你很小心的设置你的帐号模板参数，你就可以使用姓名来创建一个唯一的帐号，但是你也可以覆盖新建帐号默认设置来为特定的用户指定很多其他的选项。所有的字段必须以逗号分隔。

该逗号分隔的文本文件的每一行必须只包含一个条目。第一行是个基行包含名字和其他字段。例子如下：

```
"Mailbox", "FullName", "MailDir", “AllowAccess”
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"frank", "Frank Thomas", "C:\Mail\Frank\", N
```

注意：
在基行的字段名字被 Mdaemon 用来决定数据次序，因此可以是任意次序。每一个字段值必须在引号之内。

所有的字段值必须符合规范，如“布尔”字段必须是：y,Y,1,t,或 T。

在每个全名字段中，你可以使用首名，中名，末名，之间可以不用逗号。

在导入以后，Mdaemon 将创建 TXIMPORT.LOG，详细描述了导入的结果，列出了哪些帐号导入成功哪些没有。没有导入成功的典型原因是和现有的邮箱名字，全名，目录信息，别名，邮件列表名字之一相冲突

查看你的\API\目录下 MD-API.html 文件中 MD_ImportUserinfo( )和 MD_ExportAllUsers( )的描述。

用基行中的以下值来匹配 Mdaemon 中的帐号字段：

Field Name	Type
MailBox	string
Domain	string
FullName	string
MailDir	string
Password	string
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	bool
RemoveFromList	bool
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	string

Windows NT 安全帐号整合

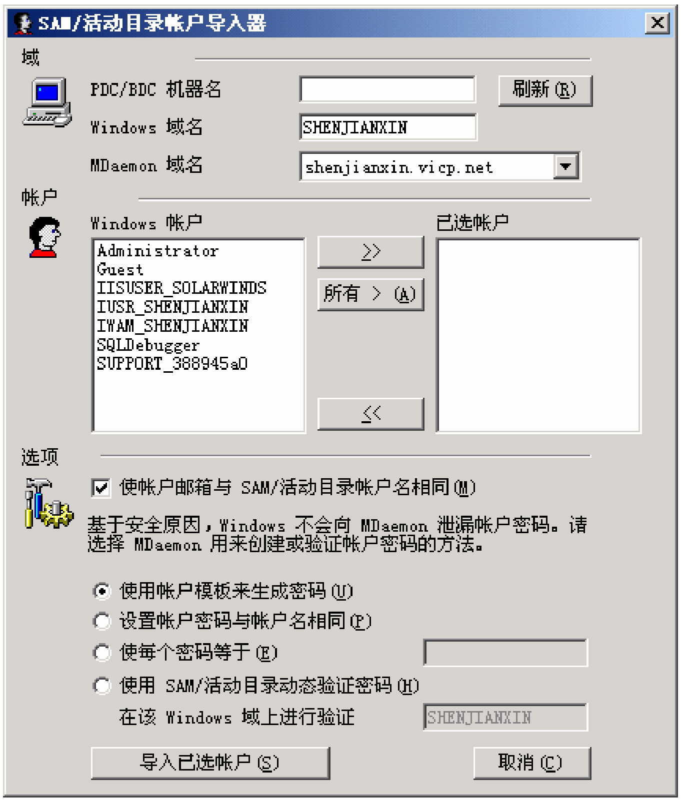
Mdaemon 支持 windowsNT 整合。这种帐号包含 windowsNT 用户数据库导入引擎，可以通过 Mdaemon 菜单选项**帐号→导入→从 NT SAM 数据库中…**另外，支持对于用户的动态认证。为帐号的密码字段指定一个 NT 域，Mdaemon 将使用 NT 域的安全系统进行动态的实时的验证。在这种机制下，在 NT 用户管理器中改变帐号的密码将直接同 Mdaemon 进行更新。因此，你的用户只需要记住一个密码就可以了。这也使得初始安装是帐号的建立变的容易很多。

重要！

帐号的安全关系，需要运行的Mdaemon必要有**SE_TCB_NAME**权限。如果此进程是以本地系统帐号运行，默认是有这个权限的。其他的情况必须要进行如下设置：

用**NT管理工具**运行**用户管理器**在**策略**菜单中选择**用户权限。注意：**你必须选择“**显示高级用户权限**”来查看**SE_TCB_NAME**权限。正确的权限，**SE_TCB_NAME**被标记为*以操作系统方式操作*,然后把这个权限加到Mdaemon所操作的这个帐号中去。如果想让帐生效，必须重起Mdaemon。
”

NT/2000帐号导入器



NT/2000服务器属性

PDC/BDC 机器名
在这里指定Mdaemon将要读取帐号数据信息的机器名字。你可以指定 \\<DEFAULT>，Mdaemon将从本地读取帐号数据信息。

刷新
单击这个按钮来刷新 NT 帐号列表。

NT 域名
输入你想要导入帐号的 NT 域名。

Mdaemon 域名
从下拉框中选择将要导入帐号的 Mdaemon 域。

帐号导入
NT/2000 帐号
这个窗口包含了从 NT 帐号数据库中收集的帐号名字列表。

已选帐号
这个窗口包含了你选择要导入的帐号名字列表。

>>
单击这个按钮把选中的帐号名字从 **NT/2000 帐号**移动到已选帐号中。

<<
单击这个按钮把选中的帐号名字从已选帐号移除。

导入选项

*使帐号邮箱和 **NT/2000** 帐号同名*
单击这个选项强制帐号邮箱使用 NT/2000 帐号名字。通过这种方法，你不必要去担心新建帐号模板的设置。

使用帐号模板来生成密码
这个选项使 Mdaemon 使用帐号模板设置来为导入的帐号生成密码。

设置密码和帐号同名
这个选项使 Mdaemon 使用帐号名字作为帐号的密码。

使每一个密码等于
这个选项为所有导入的帐号指定一个静态的密码。

*使用 **NT/2000** 动态验证密码*
这个选项可以为导入的帐号开启动态验证。对于指定一个密码，Mdaemon 使用 NT 数据库动态验证邮件客户端提供的用户名和密码。

在该 NT/2000 域上进行验证

输入 WINDOWS NT 域名，以便 Mdaemon 用来对连接进行动态的验证。**这不是域控制器的机器名。这是 NT 域的真实名字。**

注意：

当帐号被配置成利用 NT 来进行动态验证的时候，在帐号的密码字段必须是两个反斜杠加上 NT 域名，在 USERLIST.DAT 文件中明码存储。例如：一个帐号使用 ALTN 的 NT 域名来做动态验证，那么这个帐号的密码字段将包含\\ALTN。在域名前面的两个反斜杠将触发Mdaemon使用域帐号数据库要验证邮件客户端发送的用户名和密码。如果在密码前加上两个反斜杠，那是错误的，除非是被配置成使用动态验证。换种说法，你不能在在常规密码以两个反斜杠开始。以两个反斜杠开始的密码，总是被认为是使用动态验证的域名而非密码。如果有必要，在常规帐号编辑器里面输入两个反斜杠和域名是可以接受的。管理员没有必要一定要使用导入器来设置帐号来动态验证。

第二十二章

MDaemon® 中文版

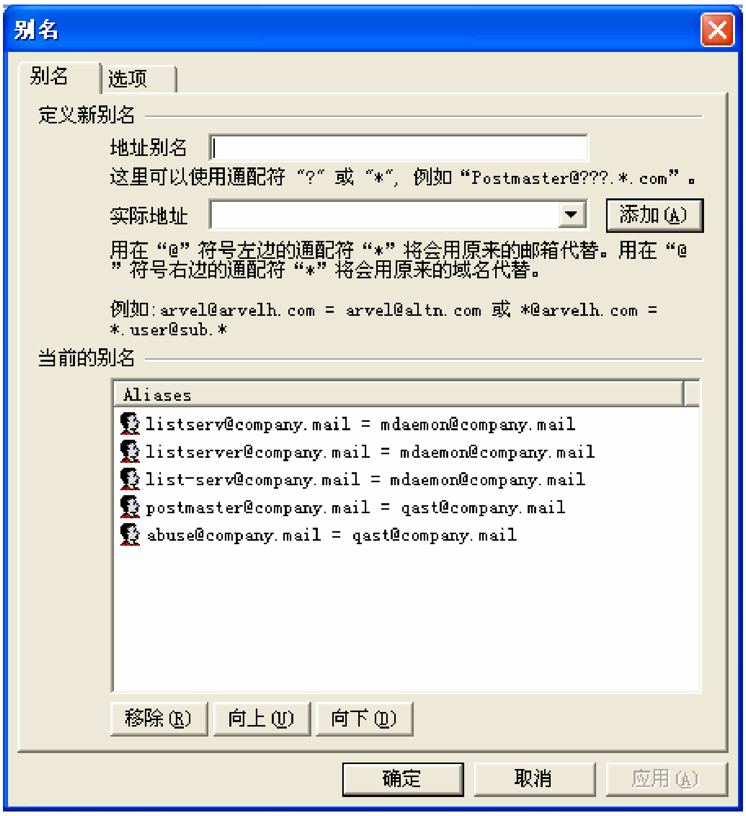
地址别名

设置地址别名

通过**帐户→地址别名**菜单来打开别名编辑器。编辑器可以为你的帐户或邮件列表创建虚拟邮箱成为可能，当为单个用户帐户或列表创建多个邮箱时，这将变得十分有用。例如，如果Frank@altn.com掌握所有的账单查询，但是你想让所有的人都发到Billing@altn.com，那么你可以创建一个地址别名，所有发到Billing@altn.com的邮件实际上会到Frank@altn.com上的。或者你可以管理多域和让所有发给Postmaster（不论域）的邮件发给某个用户。那么就可以创建别名Postmaster•*=Henry@altn.com.

因为 Postmaster 在每个邮件系统上都存在，Mdaemon 将在程序启动的时候检查别名，如果你没有创建，系统会发出一个警告。

别名



定义新别名

地址别名

输入你想别名的邮件地址，可以使用“?”和“*”的通配符。

实际地址

从下面列表中选择帐户或者在空白处键入新的邮件地址或邮件列表。这是发给相应别名时收件的实际地址。

添加

点击添加按钮来注册帐户别名请求。在地址别名和实际地址中的内容将合并到当前的别名框里。

当前的别名

该窗口包括你创建的所有地址别名。

移除

点击该按钮将移除你在当前的别名框里选定的条目。

向上

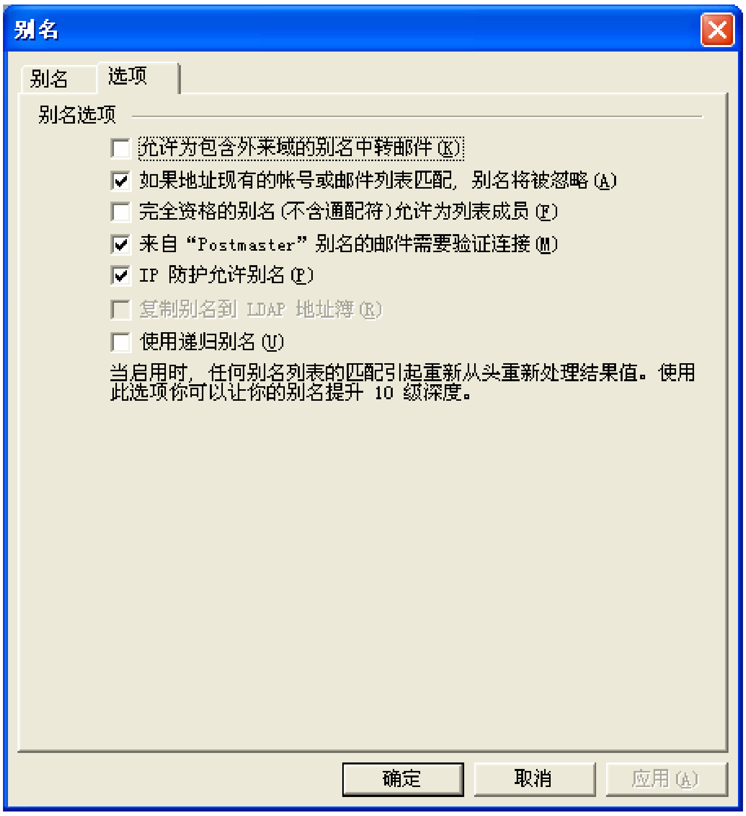
别名将会按照排列的顺序来处理的，通过选择和点击该钮，你可以将别名放到较

高的位置。

向下

别名将会按照排列的顺序来处理的，通过选择和点击该钮，你可以将别名放到较低的位置。

选项



别名选项

允许为包含外域的别名转发邮件

如果你希望 MDaemon 能为别名传递邮件，而忽略在你在中转控制中的设置

如果地址和现有的帐号或邮件列表匹配，别名将被忽略

有些时候你想为一些地址创建别名但是不想和已存在的帐户冲突。例如，你可以使用通配符来命名“*@mycompany.com=me@mycompany.com”，这会让所有包含“@mycompany.com”的邮件发到“me@mycompany.com”上，即使这个地址已经存在。但是通过选中该项可以避免。

完全资格的别名（不含通配符）允许为列表成员

如果你希望允许地址别名成为 MDaemon 的邮件列表成员，请选择该项。如果该项未被选中，那么只有真实的帐号可以成为列表成员。注意：即使选择该项，包含通配符的地址别名不允许成为列表成员。

来自 “Postmaster” “abuse” “webmaster” 的邮件需要验证连接”

需要验证来自“postmaster@...” “abuse@...” “webmaster@...”别名或帐号的邮件时钩选该选项。垃圾邮件的制造者和黑客都知道“postmaster”帐户存在，并试图通过该帐户发送邮件到你的系统。这个选项可以防止这样的情况发生。在安全 IP

防护/AUTH/…里的 STMP 验证选项里也可以设置。

IP 防护允许别名

如果你希望 IP 防护（安全 IP 防护…）允许地址别名，当检查域/IP 地址防护时，请钩选此选项。如果 IP 防护允许别名被钩选，那么当别名通过防护时，IP 防护将为其指向的地址把它转换为实际的帐户并给与允许。如果没有选择该选项，那么 IP 防护将重复出现的别名视为帐户的独立地址。不符合 IP 防护的邮件将被拒绝。

复制别名到 LDAP 地址簿

如果你想让别名被复制到 LDAP 地址簿，请选择此项。别名的复制对远程 LDAP 验证特征工作的可靠性是很必要的。如果你不使用特征，那么就没有把别名复制到 LDAP 地址簿的必要。如果你不使用远程认证，那么你可以安全的禁用该主题来节约时间。

使用递归别名

如果要处理递归别名请钩选此项。任何别名匹配将使结果值通过整个别名列表再处理——可能使别名创建十级深度。例如，你可以像这样配置：

durge@example.com = frank@example.com
frank@example.com = x@x.com
x@x.com = dwimble@my-example.net
逻辑上等同与单条别名:
durge@example.com = dwimble@my-example.net
这也意味着:
frank@example.com = dwimble@my-example.net

第二十三章

MDaemon ® 中文版

自动回复与MBF文件

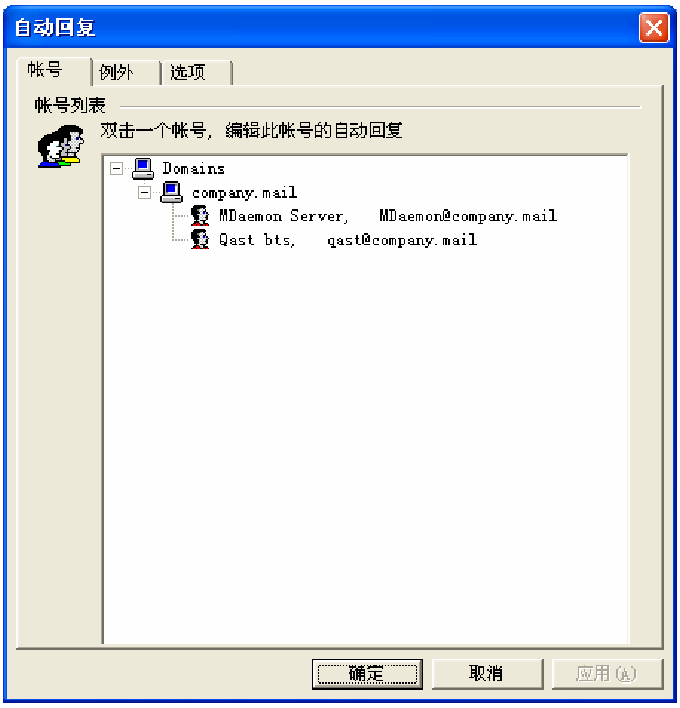
创建和使用自动回复与 MBF 文件

自动回复是一个由进入的邮件信息自动触发事件的有用工具。自动回复最常用于某人在度假、生病或无法阅读邮件等情况发生时，将用户定义的邮件回复给任何发邮件的人。使用 MdaemonV8 提供的自动回复机制，进来的邮件可以作为一个触发器来自动产生和个性化的回复。自动回复邮件文件（*.RSP）可以包含任何对 MBF 文件可用的摩板参数。

MBF 或者邮箱格式文件是和其他能接收 ASCII 文本到他们邮件流的邮件传输系统兼容的文本文件，MBF 文件其实是包含特殊格式宏集的模板文件，可以使 Mdaemon 传输 RFC-822 邮件到其他多种的基于文本的格式。使用 MBFs，Mdaemon 可以配置成对于进来的邮件进行重新格式成指定的基于每个邮箱的格式。当一封邮件发往 Mdaemon 帐号，那帐号的 MBF 文件被用来重新格式进来的邮件以便分发给用户。

自动回复

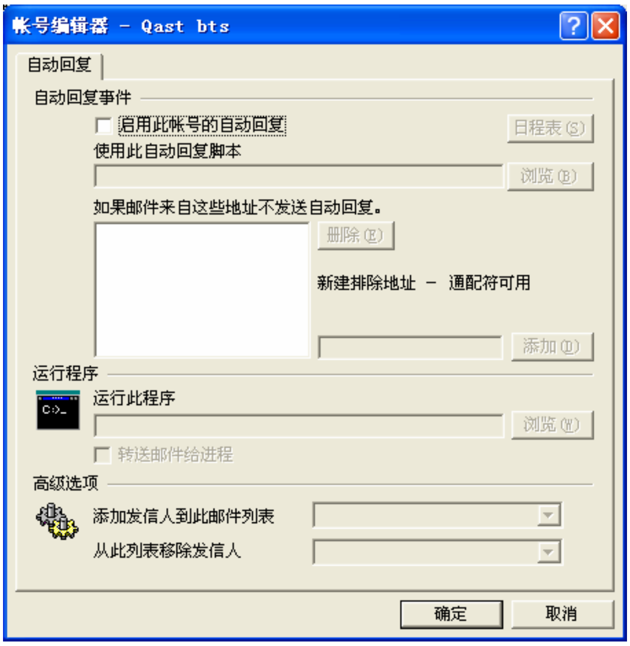
帐户



帐户列表

这个控制列出了允许自动回复的本地邮箱，双击列表里的名单可以打开相应的自动回复对话框。通过自动回复对话框可以为帐号设置自动回复。

自动回复



自动回复事件

启用此帐号的自动回复

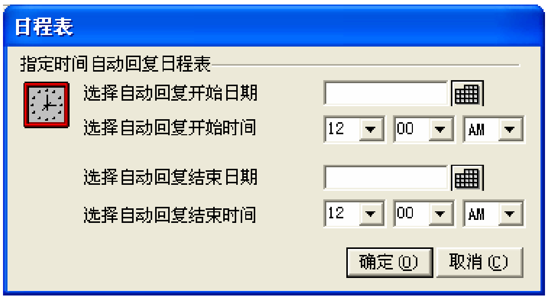
钩选这项可以激活一个帐号的自动回复。

使用此自动回复脚本

这里指定将要处理并回复给发件人的回复文件的路径和文件名（*.RSP）。该文件将首先于 MBF 文件一起通过过滤机制。任何在 MBF 文件可用的模板字符串在自动回复文件中也可用。

日程表

点击此按钮打开时刻表对话框，在这上面你可以设置激活自动回复的开始和结束日期与时间。如果你希望那个自动回复一直活动，留空此框。



如果邮件来自这些地址不要发送自动回复

这里，你可以列出你希望不包括在自动回复所发起的回复中的地址。

> 注意
> 有时候自动回复邮件发往一个地址，然后又会返回一个他自身的回复。这将会创建一个“ping-pong”效应导致邮件不断在两个服务器之间回复。你可以使用这个功能来阻止 Mdaemon 自动回复那些在这指定的地址。

删除
点击此按钮从例外地址中删除选择的条目。

添加
在新建例外地址文本框中输入一个地址，点击此按钮来添加它到例外地址列表中。

新建排除地址---通配符可用
如果你希望那个添加一个地址到例外地址列表，在此输入并点击添加按钮。

运行程序

运行此程序
此区域给一个程序指定完整路径和文件名，此程序将会在新邮件到达指定邮箱时启动。必须确保这个进程完全终止，或者在后台运行。可选的命令行参数可在执行路径后面添加。

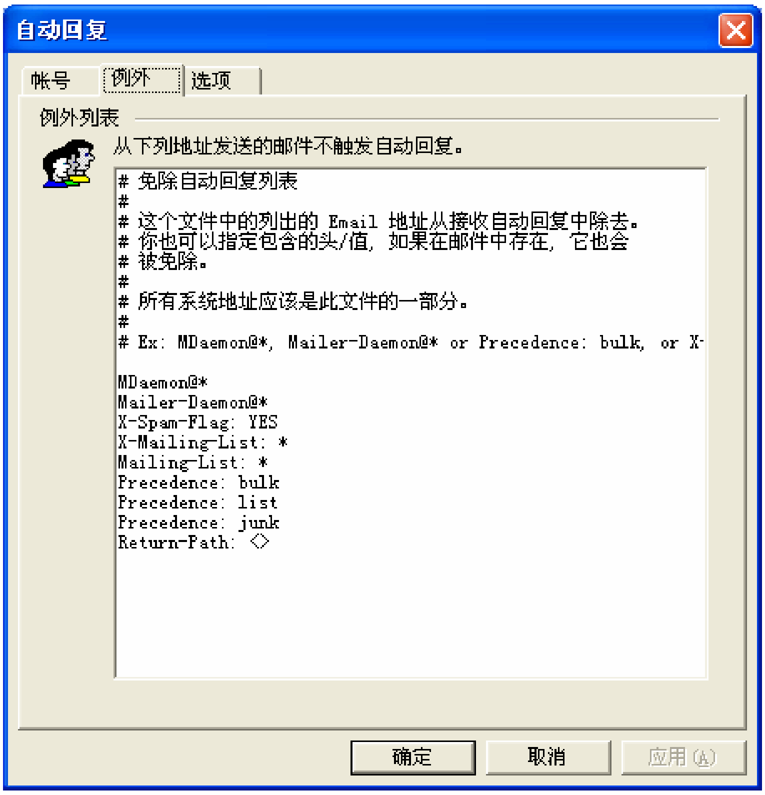
高级选项

添加发信人到此邮件列表
如果在此区域输入邮件列表，那么邮件信息的发送者将会被自动添加进邮件列表。对于创建自动列表来说，这是一个非常便利的功能。

从此列表移除发信人
如果在此区域输入邮件列表，那么邮件信息的发送者将会被自动从指定邮件列表中删除。

> 提示
> 自动回复事件总是被远程邮件所触发。如果是来自本地用户，那么是否触发自动回复在**杂项对话框**进行设置。这个选项是：*自动回复由本地和远程邮件触发*，开启这个选项，你希望本地邮件也会触发自动回复。

例外列表



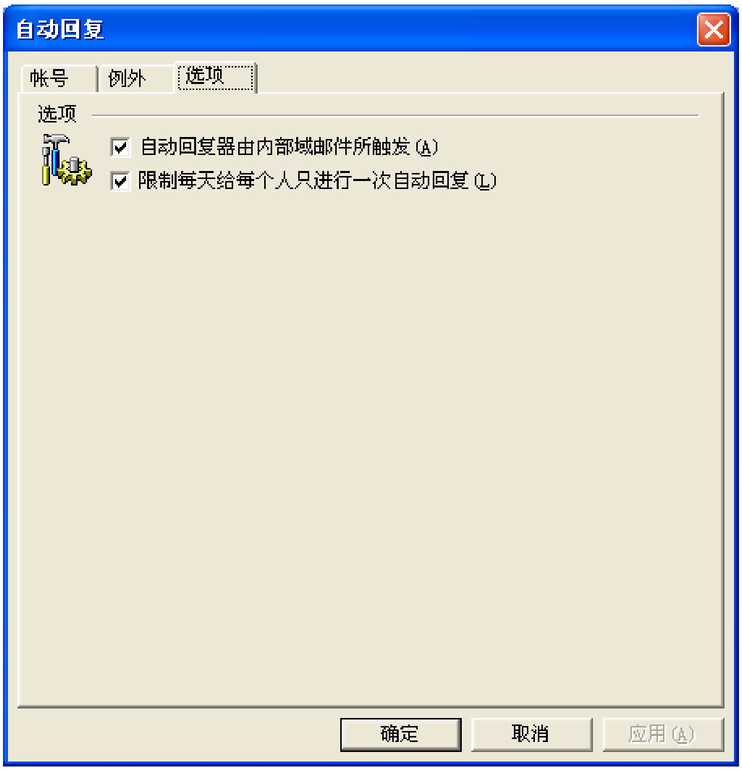
例外

使用下列例外列表将设置全局自动回复例外——从列表内所发来的邮件将不做任何回复。邮件地址和邮件头和值组合可以包含在列表。每一行输入一个地址，或邮件头和值，允许通配符。

注意

所有的系统地址（如.mdaemon@*,mailer-daemon@*,等等）应该在此列出以避免邮件循环和其他问题。

选项



选项

自动回复器由内部域邮件所触发

如果你希望本地邮件启动自动回复，请钩选此项。

限制每天给每个人只进行一次自动回复

钩选此项，将限制自动回复生成器每天只给每人只进行一次自动回复。这可以防止一个人收到多余的自动回复邮件。

创建自动回复脚本

自动回复脚本定义了作为自动回复事件返回的邮件。他们和构造 MBF 文件差不多，可以包含一些宏。然而一些附加的宏被提供允许你创建更强大的自动回复邮件。

除了为 MBF 文件定义的模板参数外，自动回复脚本可以使用任何或所有下列的宏，可以覆盖源文件的值：

%SetSender%

ex: `%SetSender%=mailbox@host.org`

Mdaemon将认为是该地址发送了原始邮件。

%SetRecipient%

ex: `%SetRecipient%=mailbox@host.org`

设定接收自动回复的邮件地址，而不管发件人是谁。

%SetReplyTo%

ex: `%SetReplyTo%=mailbox@host.org`

设置 RFC-822 回复地址。

%SetActualTo%

ex: %SetActualTo%=mailbox@host.org

改变该邮件Mdaemon认为的实际收件人。

%SetSubject%

ex: `%SetSubject%=Subject Text`

替换邮件主题值。

%SetMessageId%

ex: `%SetMessageId%=ID String`

改变邮件的 ID 字符串。

%SetPartBoundary%

ex: `%SetPartBoundary%=Boundary String`

改变邮件的局部分界线。

%SetContentType%

ex: `%SetContentType%=MIME type`

改变Mdaemon认为的邮件内容类型。

%SetAttachment%

ex: `%SetAttachment%=filespec`

强制Mdaemon在新产生的自动回复邮件上附加一个指定文件为附件。

自动回复脚本例子

一个典型的自动回复脚本 VACATION.RSP：

Greetings $SENDER$

You’re message regarding ‘$SUBJECT$’ won’t be read by me because I’m on vacation so LEAVE ME ALONE!

Yours truly (yeah right!),

$RECIPIENT$

这个 VACATION.RSP文件在Mdaemon的第一个版本中就有了。 这个例子的脚本使用了为MBF开发的宏。使用上表中定义的宏，你也可以控制在自动回复脚本处理和回复给发件人的时候，产生哪些邮件头。

让我们对老的VACATION.RSP文件进行修改以加入一些新的宏：

Greetings $SENDER$

You’re message regarding ‘$SUBJECT$’ won’t be read by me because I’m on vacation so LEAVE ME ALONE!

Yours truly (yeah right!),

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$

%SetAttachment%=c:\windows\bugoff.exe

用这个模板生成的新邮件将有个自定义的主题，还有个指定文件为编码为 MIME 的附件。

%SetSubject%=RE: $SUBJECT$ 是这样处理的：

1. $SUBJECT$部分将被原始邮件的主题文本替代。这将使这个值等于

%SetSubject%=RE: Original Subject Text。

2. MDaemon 将用新的值替代original subject,从那时起，任何调用$SUBJECT$的主题字段将会返回一个新的值。

第三部分

MDaemon ® 中文版

附加的MDaemon的功能

第二十四章

MDaemon ® 中文版

邮件列表

使用MDaemon的邮件列表功能

邮件列表有时候称之为邮件组或者分发列表，允许多组用户地址被组合起来就好象他们共享一个公共邮箱，发送到列表的电子邮件的副本分发到邮件组里的每一个人。列表可以包含本地和远程用户，可以是公开的或是保密的，适中的或敞开的，以分类发送或是常规形式发送或者更多。

邮件列表编辑器

邮件列表编辑器用于创建和维护邮件列表。可从**列表 – 新建列表…**或**列表 – 编辑列表…**菜单进入选项。

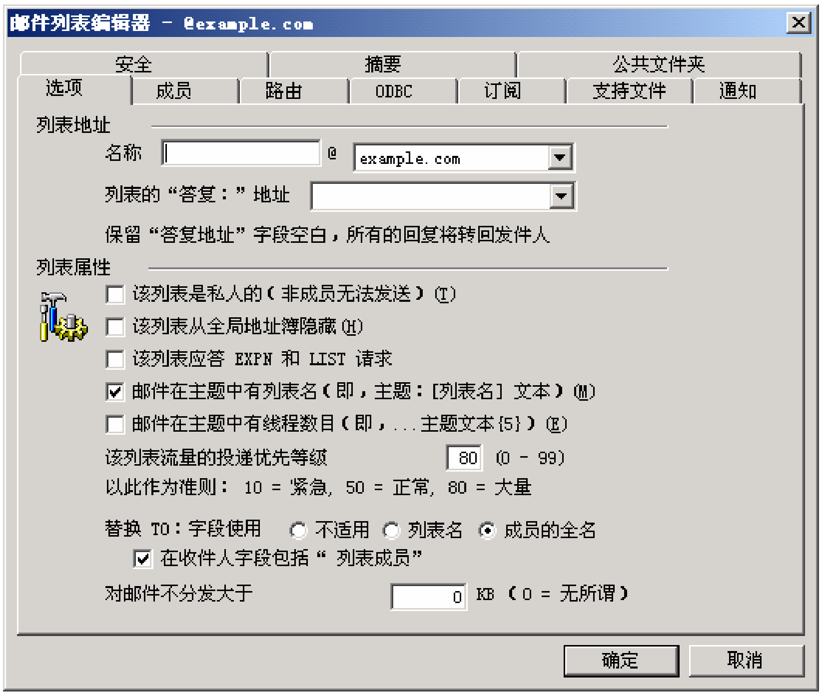
创建新的邮件列表

当选择**列表---新建列表**菜单选项，邮件列表编辑器将会打开一个新的列表。创建新列表所需参数仅为为其命名和指定其归属的域名。其它选项则保留默认值，在创建列表时您可改变这些参数也可以下次编辑时再进行改变。

修改现有的邮件列表

选择列表--编辑列表…菜单选项打开邮件列表对话框，这个对话框用于选择您希望修改的邮件列表。当您从对话框中选中一个列表后，该列表会被打开以供编辑或查看。

选项



列表地址

名称

为邮件列表命名并从下拉列表框选择所属域。发送到这个列表的邮件将使用所指定的名称和域（如：mylist@mydomain.com）.列表的名称中不能包含“！”或“|”

列表中的“回复-至：”地址

输入一个邮件地址，此地址为您所希望邮件定向回复至本列表的地址，是任何回复至本列表的邮件直接到达的地址。如果您希望回复到本列表的邮件发送至一个可选地址，也可以键入一个除本列表名以外的地址，或者从下拉列表中选择。如果此栏空白，则所有回复的邮件将退回至发件人邮箱。

列表属性

此列表为私人列表（非成员无法发送邮件）

当此功能激活，列表将只允许成员发送邮件。来源于非成员始发的邮件将被删除。

此列表对于全局地址簿为隐藏

点击此选项，从WorldClient 和LDAP公共地址簿里隐藏此邮件列表。

此列表响应EXPN和LISTS请求

如果选择此选项,在邮件处理过程中，此列表中的成员会被告知响应EXPN或LISTS命令。否则，此列表成员将会保持在不公开状态。

邮件信息在主题中有列表名

此项设置使Mdaemon将列表名字用方括号包起来（如[ListName]）并将其添加至主题的起始部分：在所有发送给列表的邮件中。

邮件在主题中有线程号（例如…主题文本[5]）

这个选项允许你切换在列表邮件的主题栏是否显示线程号。他们被添加到主题栏末尾。按标题名称排列您的收件箱，您的邮件则会按时间顺序排列。

本列表发送中的优先等级

在此控制器中键入数字0-99。此数值表示在邮件发送过程中相关的排列顺序。数值越低，邮件的重要性越高，他在一个邮件队列中排列也更靠前。
赋值标准：10=紧急，50=正常，80=大量

使用无，列表名，成员全名替换"发送至："

但凡MDaemon接收到发送给列表的邮件均使用这些项指定哪个地址将会显示在发送至字段。
无-当您选择无时，MDaemon将不会改变地址的显示。包含在发送到：字段内地址的显示与发送邮件键入的发件人地址完全相同。
列表名-此选项在发送到：字段中显示邮件列表地址
成员全名-当您选择此选项，发送到：字段将包含邮件接收列表用户的全名和邮件地址，如果全名不详，则仅包含邮件地址。

注意
当"MDaemon将分解列表邮件"被选择显示在邮件列表编辑器的路由选项中用户名选项才能被选择。当您选择"发送一个单一的副本"，MDaemon将会默认为列表名选项。

在发送到：字段内包含"[列表名]列表用户"

一旦此特性被激活，"[列表名]列表用户"将会被显示在邮件信息的发送到：字段的"真实姓名"部分中。

注意
不是所有的电子邮件用户都支持在邮件信息的发送到：字段中显示"真实姓名"这一功能。不支持的用户在"以...替换发送到：字段"特性中只显示真实的邮件地址。

不发送长于XX字节的邮件

此控键进一步限制了从邮件列表内接收的邮件的大小。大于所限制字节的邮件都将被发送至不良邮件目录里。

成员

当前成员帐号

此功能可显示当前注册于此列表的成员数并将其罗列在以下方框中。每一个成员都需表明其成员“类型”：普通，摘要，只读或仅发送。

移除

此按键将删除“当前会员”列表里的选定的条目。

摘要

选择一个成员,点击此按键使之成为“摘要”用户。详见**摘要**(386页)了解更多的摘要邮件信息。

只读

选择一个列表成员后点击此按键使其状态更改为“只读”。他们仍可从列表接收邮件但不可发送邮件至列表。

仅发送/无邮件

选择一个成员后点击此按键可使之成为“仅发送”用户。他们可发送邮件至列表但不能接收。

新成员邮件

键入您希望添加到邮件列表的地址。邮件地址不能包含“!”或“|”。

新成员实名

在此字段内输入成员的姓名，在选项标签上选定“用成员全名替代发送至：字段”选项，这个名字将会出现在邮件发送至：字段。

普通，摘要，只读，仅发送

点击以上选项选择您所希望的新成员邮件地址属性。

添加

此按键可向现有用户列表添加新用户邮件地址

默认值
选择任一选项（普通，摘要，只读，仅发送)并点击“默认值”按键,则新用户的此栏的默认值即为所选项。

导入
点击此按键从文本文档中导入列表成员,文档由逗号分隔各字段。每个条目必须在它自己的线格里且所有字段必须由逗号分开。此外，文档第一行(基线)必须罗列此字段的名称和在余下行中所显示的各字段的顺序。其中一字段必须叫“EMAIL”并包含邮件地址。还应有一名为“FULLNAME”的可选字段包含列表成员的名称。其余所有字段导入系统都不予理会。

例如：

“Email”, “FullName”, “Address”, “Telephone”
frank@altn.com, “Frank Thomas”, “123 Frank St”, “817.555.1234”

被导入的成员不会收到列表的欢迎信息包,且导入程序将不会确认成员副本。

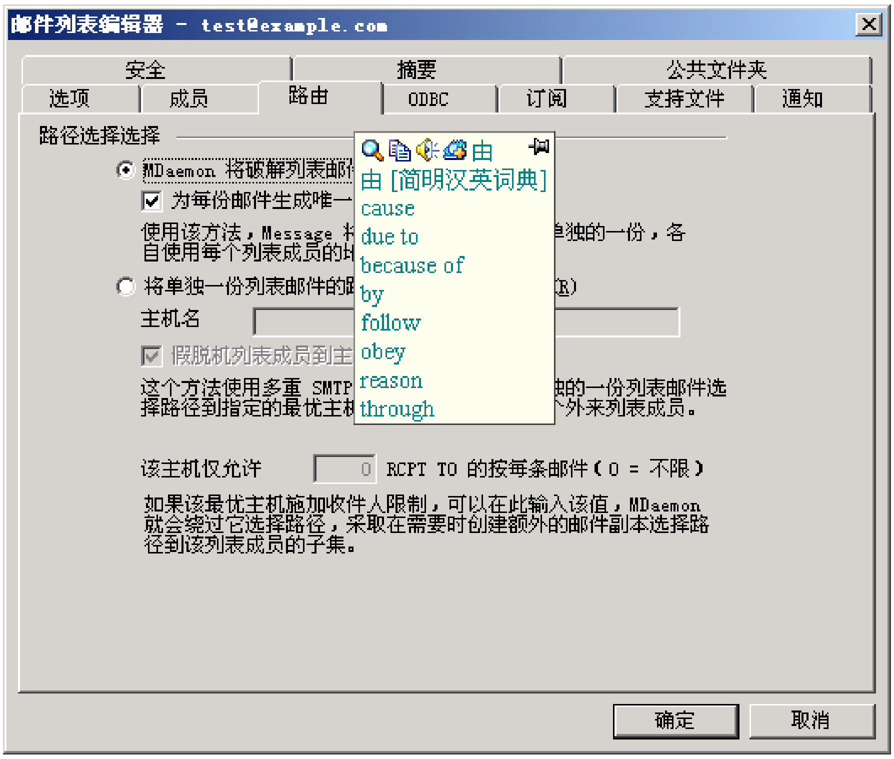
从列表成员中自动移除废弃地址
一旦此功能被激活，在 MDaemon 发送邮件过程中,若遇到永久性致命错误,MDaemon 将会从列表用户中自动去除该地址。当邮件被移动到重试系统并在该系统内过有效期，该邮件地址也被视为“坏死”地址并被自动删除。

注意
只有当远程邮件服务器拒绝接收邮件信息时,“自动去处坏死地址”按纽才起作用。当你已经将 MD 配置为“破解”邮件列表（P370）且不使用 smart 主机时，此功能才能使用。如果您将列表邮件发送至 smart 主机时，请阅读以下增强的列表修改（Enhanced List Pruning)了解更多信息。

增强列表修改
当*自动去除坏死地址*…选项启用，您已为列表邮件指定了一本地邮箱作为回邮路径(详见通知标签中的退回邮件控键)，每一天午夜，MDaemon 会试着从被退回的邮件中分析有问题的地址并除去不能送达的用户。这将有助于提高从邮件列表中筛选无效地址，特别是当您不是直接发送邮件信息而是发送至 smart 主机时。

在其它选项卡（P292）中的其他键上有两个控键与此功能有关。其中一个可以删除不包含 parsable 地址的被退邮件。另一个将会保存所有由于列表成员地址删除而无法处理的邮件。

路由



MDaemon 将分解列表邮件

如选择此项，单独的列表邮件将会被创建并被发送至各列表成员。这将会导致众多的单独的邮件被创建并影响服务器的运作。此选项适用于 15 或以下成员的邮件列表。

为各副本生成唯一的邮件 ID

当 Mdaemon 分解列表邮件时，它将为每个成员创建一个独立的邮件副本。如果用户需要，MDaemon 可以确保每一个列表邮件都包含一个唯一的 ID。

发送一个单独的列表邮件副本到此 smart 主机/主机名

如此项被选择，MDaemon 将会单独发送每一个列表邮件的副本至一个特定的 smart 主机。此程序在 SMTP（简单邮件传输协议）过程中，调用多重（multiple) RCPT TO 命令和特定 host 一起使用。

spool 列表邮件至主机时忽略误差

由于一些 smart 主机会拒绝队列或 SPOOL 某些域的邮件，已选择的发送路径会引发众多问题。从 smart 主机退回的一个错误代码会造成 MDaemon 发送任务的异常中断。如果这个功能开启，MDaemon 将忽略上述错误代码从而允许已接受承担风险的成员接受到列表邮件。

主机允许（XX）RCPT TO 的每一个邮件（0=无限制）

当您试图通过主机发送单个邮件副本时候，一些主机将会限制他们接受到的 RCPT TO 语句的数量。如果您在此控键内设定了限制，MDaemon 将会通过创

建附加邮件副本和将列表划分成更小的群组来遵守所设定的限制。MD 将会将邮件发送至上述群组从而避免超出限制范围。这与“分解”列表的功能相似，但是是分解成群组而不是单个。

ODBC

现在，您可以将您的邮件列表中的成员列表保存在一个 ODBC 适应的数据库中。邮件列表编辑器的 ODBC 标签是用来为 MDaemon 选择数据源，图表和字段映射使之能链接到列表。当邮件发送到你的列表时，将会有一个或多个 SQL 询问自动执行，产生的邮件地址也会作为列表成员之一。

您可在数据库中使用您选择的任一 ODBC 适应的数据库应用程序来增加，删除以及更改您的列表用户。

当前 ODBC 属性

这部分显示了你现有的为邮件列表设置的 ODBC 属性。它显示了数据库的地段匹配和 SQL 查询，你使用这些配置来指出每一个成员的会员资格状态（如普通，只发送，只读，或摘要模式）。
这部分显示了您为邮件列表设置的现有 ODBC 属性。它显示了数据库字段映射和 SQL 查询，您可使用这些设置来指定各成员的类别（如，普通，仅发送，只读和/或摘要模式）。

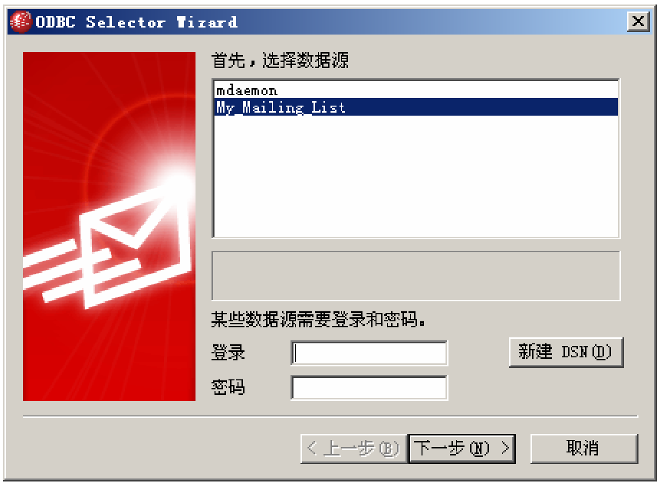
连接到新的 ODBC 源

点击此键打开 ODBC 选择向导选择您希望在邮件列表上使用的系统数据源。

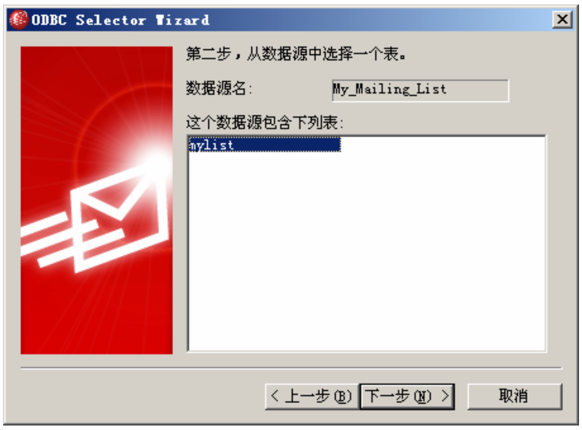
为邮件列表选择和配置一个ODBC系统数据源

将 ODBC 可存取数据库与邮件列表一起使用：

1. 打开邮件列表（**Ctrl+E 或列表—编辑列表**）切换到 ODBC 键，点击“**连接到新 ODBC 源**”打开 ODBC 选择向导。
2. 选择您希望用于邮件列表的“**数据源**”。如果列表中没有兼容的数据源，通过下文所说明的“**创建一个新的系统数据源—P375**”的步骤来创建一个新的数据源。
3. 点击“下一步”

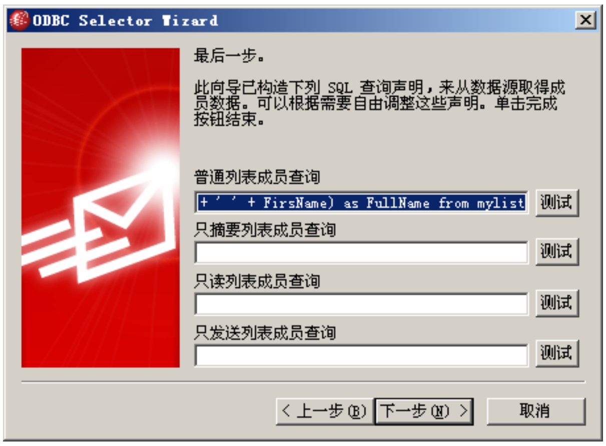


4. 数据源必须包含至少一个图表和填写地址和姓名的空格。如果此数据源包含一个或更多符合要求的图表，选择合适的图表并点击“下一步”。若不符合，点击“**取消**”键来退出 ODBC 选择向导，然后选择您自己的数据库应用程序来添加图表至相应数据库。



5. 使用下拉列表框指明与**邮件地址，姓，名**对应的图表空格。点击“**下一步**”

6. ODBC 选择向导会根据您在第五步中的选择来建造一个 SQL 询问语句。MDaemon 会用其从您的数据库中检索普通列表成员数据。您可编辑此状态为希望检索到的，并在剩余的控键中包括进其余询问语句，使用户在摘要模式中接受邮件，也可指定用户类别为“只读”或“仅发送”。除各控键外，还有一个测试键用于测试询问语句来确定检索出的确为所需数据。

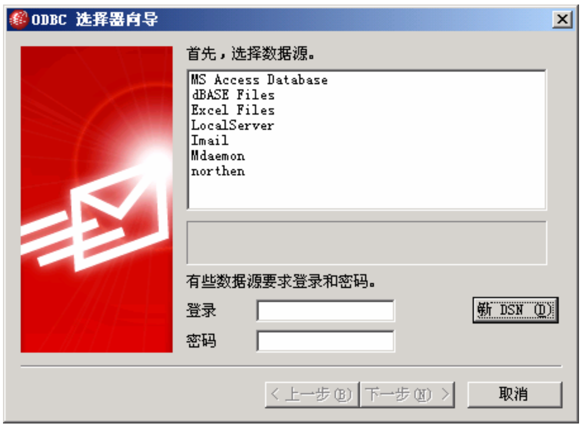


7. 点击下一步，并点击完成

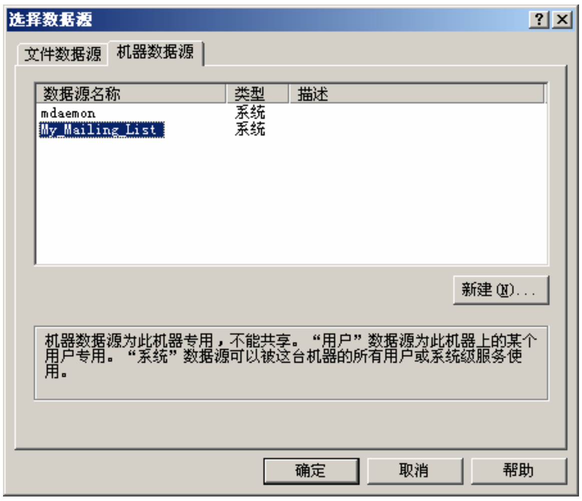
创建一个新的系统数据源

通过邮件列表创建一个新的 ODBC 系统数据源供使用：

1. 打开邮件列表(**Ctrl+E 或列表-编辑列表...**)切换至 ODBC 选项卡，点击“**连接到新 ODBC 源**”来打开 ODBC 选择向导。

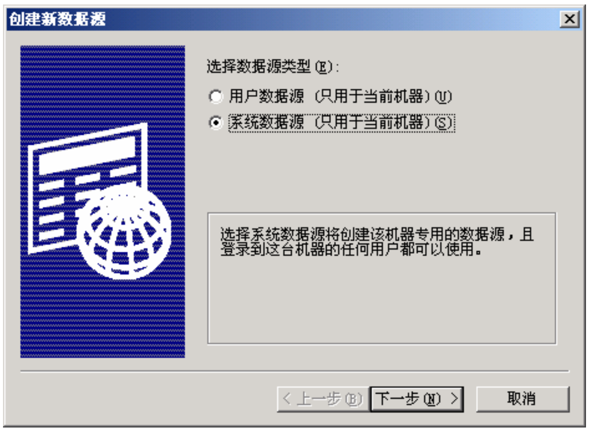


2. 点击“**新建 DSN**”打开选择数据源对话框。切换至“**机器数据源**”选项卡。



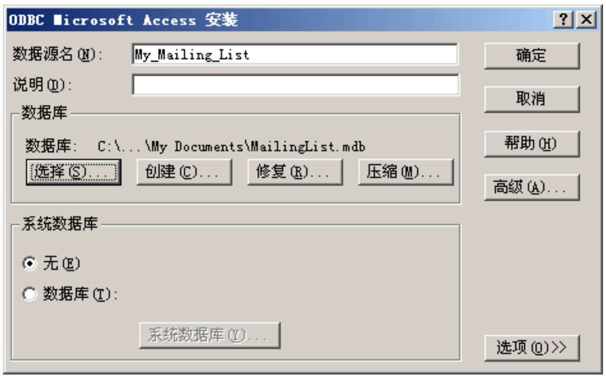
3. 点击“**新建**”打开新建数据源对话框。

4. 选择“**系统数据源**”点击“**下一步**”



5. 为将建立的数据源选择“**数据库驱动程序**”并点击“**下一步**”

6. 点击“完成”来显示驱动细节的对话框。此对话框的样式会根据你所选的不同驱动程序而改变。(以下为微软公司 ACCESS 建立对话框)

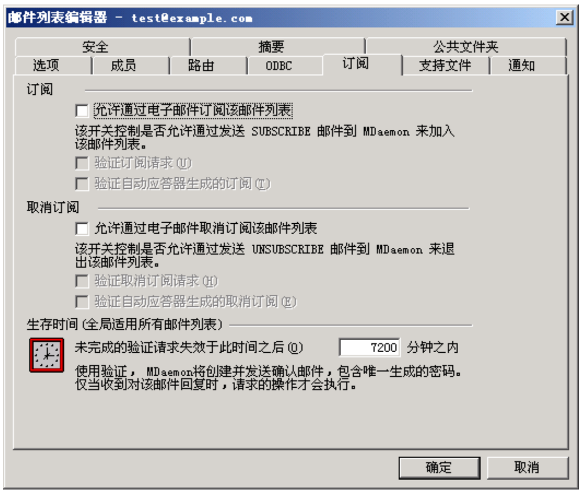


7. 为您的新数据源指定一个**数据源名**，并根据驱动细节对话框提供其它所需的信息（如创建或指定一个数据库，选择一个辞典或服务器，等等）

8. 点击“**完成**”关闭驱动细节对话框。

9. 点击“**完成**”关闭所选数据源对话框。

订阅



订阅

允许通过电子邮件订阅该邮件列表

该开关控制是否允许潜在成员通过发送订阅邮件到 MDaemon 来加入邮件列表。

验证订阅请求

设定该开关后，MDaemon 会验证订阅请求。系统会完成此验证并为验证程序生成一个唯一的密码串。一封包含此密码的邮件会发送至潜在成员。一旦该成员回复此邮件，MDaemon 就会将此成员添加至邮件成员列表。

验证自动应答器生成的订阅

当您通过"*添加发送者至列表邮件*"自动应答器添加成员时希望验证订阅则点击此选项。

取消订阅

允许通过电子邮件取消订阅该邮件列表
此开关控键允许成员通过电子邮件取消订阅该邮件列表

详细：

远程服务器通过邮件监控-P432

验证取消订阅请求
此开关的设定可使 MD 验证所取消的订阅请求。详见"*验证订阅请求*"中关于所用机构（mechanism employed)的讨论来完成此验证。

验证自动应答器生成的取消订阅
当成员由"*将成员从此列表删除*"自动应答器选项被删除时希望验证此取消订阅则点击此选项。

生存时间(全局适用于所有邮件列表)

未完成的验证请求失效于 XX 分钟之后
当某人被订阅或被取消订阅，此时间为订阅（或被订阅）失效前的确认命令应花费的时间。MDaemon 会生成一个确认邮件并发送至被订阅的地址。收信人必须在此订阅命令失效之前的规定时间内回复此邮件。这个时间值是全局化的；应用于所有的 MDaemon 邮件列表而不只是现正被编辑的这一个。

订阅邮件列表
订阅一个邮件列表，将邮件地址发送至某个域的 MDaemon（或其别名）所控的邮件列表，把订阅要求写在邮件正文的第一行。例如，altn.com 的邮件列表名为 MD-SUPPORT。您可以通过构造一个邮件地址至"madaemon@altn.com"来订阅列表并设置一个数值：SUBSCRIBE MD-Support@altn.com 作为邮件正文的第一行。邮件的主题无关紧要，可略写。

如何完成此订阅和其他控键的详细信息，请查阅：

远程服务器通过邮件监控-P432

您也可利用 MDaemon 的自动应答器特性自动订阅列表用户，当用户发送邮件至自动应答器时，帐户被激活。详见 P353 了解此特性详细信息。

最后，新的 MDaemon8 特性为订阅功能，其可使 MD 承认"（list)-subscribe@domain.com"和"（list)-unsubscribe@domain.com"格式的邮

件地址为用户提供更便捷的方式假如及退出其邮件列表。例如：假设您的列表名为 MyList@altn.com。他人可以通过发送邮件至 MyList-Subscribe@altn.com 和蔼 MyList-Unsubscribe@altn. com 来订阅和取消订阅其邮件列表。邮件的内容和标题无关紧要。另外，当此特性被激活，MD 会插入以下标题至所有列表邮件：

List-Unsubscribe:<mailto:<list>-Unsubscribe@domain.com>

一些邮件客户程序可看到此标题并自动生成“UNSUBSCRIBE”按钮给用户提供选择。

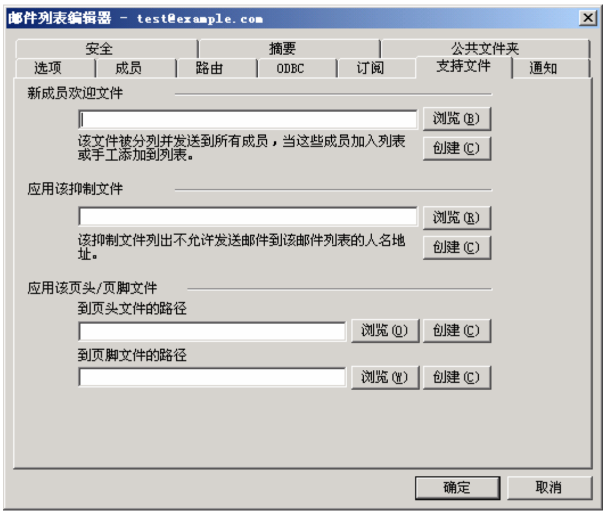
此新功能在其他选项卡的其他键上（P292）

注意

有时，用户会发送指令至列表本身而不是 MD 的系统帐户来订阅或取消订阅列表。这将会导致命令被发送至列表而不是用户被订阅或被取消订阅.为防止此类邮件被发送至邮件列表,可启动其他选项卡中系统制表符的“*程序前邮件列表邮件*”控键。（P285）

当那些包含列表名的命令被发送至列表地址而不是系统帐户时，会导致这些包含订阅，取消订阅以及结束命令的邮件被拒收。

支持文件



新成员欢迎文件

如果启用本功能，当新成员完成订阅后，以下所罗列的文档将会被处理并将内容发邮件至所有新成员的邮箱。您可以在新成员欢迎文件中使用以下的宏指令：

PRIMARYDOMAIN	该指令扩大为 MD 的第一域名，被指定在第一域配置对话框中（点击新建-第一域）。
PRIMARYIP	该指令将返回 IP 和 MD 的第一域
MACHINENAME	该指令在第一域对话框的域制表符上返回“计算机名”内容。
LISTEMAIL	显示列表的邮件地址。如：MyList@example.com
LISTNAME	显示邮件列表名。如：MyList
LISTDOMAIN	该指令返回邮件列表域。如：example.com

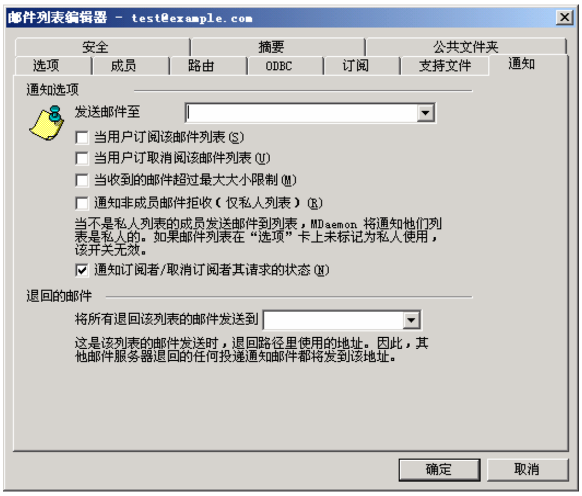
应用该抑制文件

如果启用本功能，所列的文档将会用于禁止某些用户发来的邮件。相关信息详见禁止文档的禁止地址（P168）

应用该页眉/页脚文件

此处所列的文档内容将会作为列表邮件的页眉页脚文件。

通知



通知选项

发送邮件至

当所选项起作用时，此项显示出将被发信通知的地址。

当用户订阅该邮件列表

选择此项，每当有人订阅本邮件列表时，通知书将会发送到指定地址

当用户取消订阅该邮件列表

选择此项，每当有人取消订阅本邮件列表时，通知书将会发送到指定地址

当收到的邮件超过最大大小限制

选择此项，每当有人发送至邮件列表的邮件大于列表的最大限度时，通知书将会发送到指定地址。改邮件会被移动至不良邮件目录。

通知选项

通知非成员邮件拒收(仅私人列表)

当不是私人列表的成员发送邮件到列表,MD 将通知他们列表是私人的。他们将会被收到关于如果订阅列表的说明书。

通知订阅者/取消订阅者其请求的状态

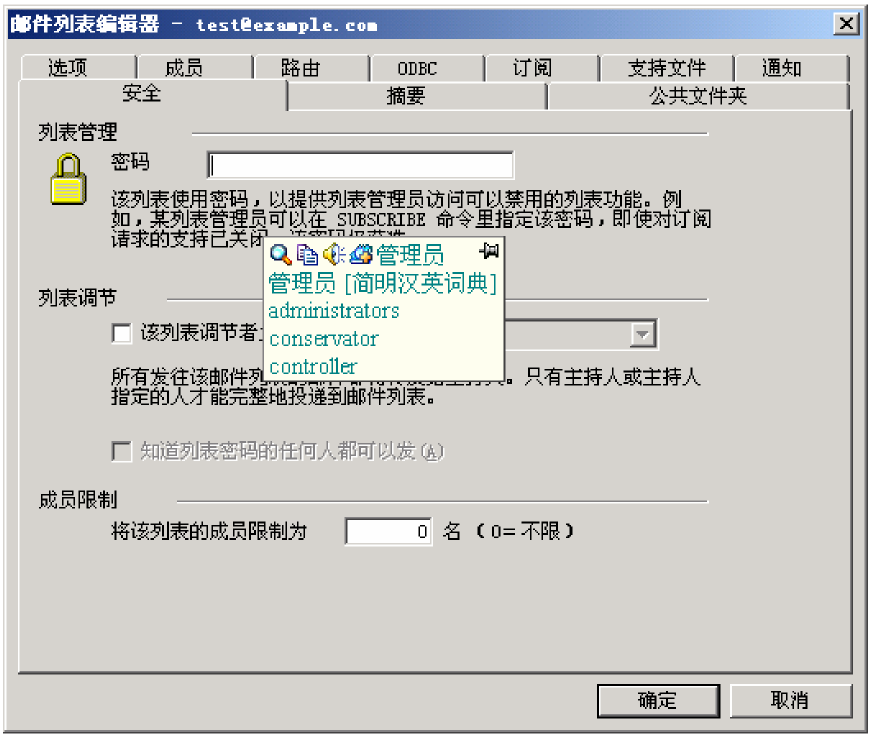
当该检验选项激活，MD 会发送一封完整的通知邮件给订阅或取消订阅的用户。

退回的邮件

将所有退回该列表的邮件发送到

此选项卡中您可指定谁将接受所有退回列表的邮件。举例说明，一个邮件列表中有 100 个收件人，这 100 个之中一般会有 10-20 个无法投递的地址，可能是由于地址改变，服务器故障或其它原因。STMP 系统将生成和退回给发件人关于这些无法投递的地址的状态的邮件。您可以设定谁应收到这些通知邮件。您还可指定如果 MDaemon 将邮件列表置入邮件流（STREAM），可设定无人接收邮件通知。这样一来，退回邮件就不可能了。

安全



列表管理

密码

在此控键中输入进入列表的密码。

列表调节

该列表调节者为

如果设置本选项，列表将会允许被指定用户调节。被调节的列表会将所有邮件转发至调节者。只有调节者一人可将邮件提交或转发至列表。

知道列表密码的任何人都可以发

该选项如被选中，调节者可发配一个密码给邮件列表。所提交至已调节列表的邮件将不会再被调节。已调节列表在标题的第一行有 X 字母开头的密码。也就是说，邮件会被即刻发送就好象它发送自调节者。

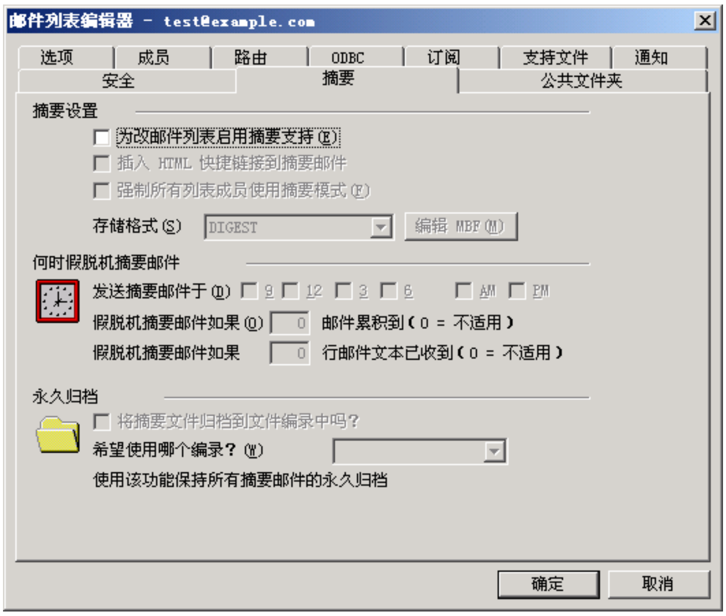
举例说明：绕过调节者出现在已调节列表上的称之为 MDSUPP，他的密码为 ALTN，那么，就将 ALTN 作为邮件标题的头四个字母。

成员限制

将改列表的成员限制为 X 名（不设上限）
您可以设置一个无上限的人数，允许订阅邮件列表，如果您不希望限制订阅的人数，键入 0

注意
此限制只适用于那些能通过订阅命令订阅列表的用户。此限制不能通过 MD 界面实现订阅，也不能通过伴随列表密码的订阅命令实现。

摘要



摘要设置

为改邮件列表启用摘要支持

此控键决定了邮件列表是否支持邮件摘要。当摘要支持启用，每封发送至邮件列表的邮件副本将会被归档。被选来从列表接受摘要格式邮件的列表用户将会发送这些压缩的归档邮件且便捷使用索引格式。

插入 HTML 快捷链接到摘要邮件

当该控键激活，MDaemon 会转换所有发现的 URLS 在摘要邮件内给超文本链接。

强制所有列表成员使用摘要模式

默认值的设定为，列表用户可调控所接受到的 TRAFFIC 为摘要模式还为普通模式。此控键强制所有成员无论自己选择何种模式都需使用摘要模式。

存储格式

选择 MBF 文档使置入摘要的独立邮件保持一致。默认值为 DIGEST。MBF 文档能提供典型的函数性能与大多其他的邮件列表软件媲美。了解如何创建 MBF 文档的详细信息，详见*创建和使用 MBF 文档*-P359

编辑 MBF

点击此按扭编辑*存储格式*控键中列出的邮箱格式文件。

何时假脱机摘要邮件

发送摘要邮件于上午或下午 ***9，12，3，6*** *时*

邮件列表摘要必须间隔性地发送至那些被设定用摘要格式接受邮件的列表用户。这些控键允许您如此设置。

假脱机邮件摘要邮件如果邮件累计到 ***X*** *（* ***X*** *不能为* ***0*** *）*

有时，需根据积累的邮件数量而不是（或附加）特定时间向列表用户发送摘要邮件。此控键允许您指定在发送摘要给摘要模式的列表用户之前所积累的邮件数量。

假脱机邮件摘要邮件如果 ***X*** *行邮件文本已收到（* ***X*** *不能为* ***0*** *）*

此控键将导致摘要增长至许多文本行时，被立即发送出去。

永久归档

将摘要文件归档到文件编录中吗？/使用哪个编录？

该控键允许您设置摘要信息至文档目录以使反馈的摘要可被收集。MD 将会为没一个摘要生成一个唯一的归档名并将其放入您指定的目录内。

了解如何使用目录的详细信息，详见

创建一个新目录-P389

公共文件夹

支持公共 IMAO 文件夹是 8.0 的新特性。公共文件夹是提供给 IMAP 用户额外的文件夹，他与 IMAP 个人文件夹有着不同之处，后者是典型的仅为个人用户所配备的。该控键被用来使所有发往本列表的邮件被自动复制到您其中一个公共文件夹。欲知关于公共文件夹更详细的信息，详见 P114。

公共文件夹

将列表邮件复制到公共文件夹

如果您希望此列表邮件除正常发送之外还被复制到您其中一公共文件夹，请启用本功能。

选择公共文件夹

点击您希望联合列表邮件一起使用公共文件夹。

新建

点击新建按扭建立新的公共文件列表为列表所使用。这会使公共文件对话框（P114）打开。

第二十五章

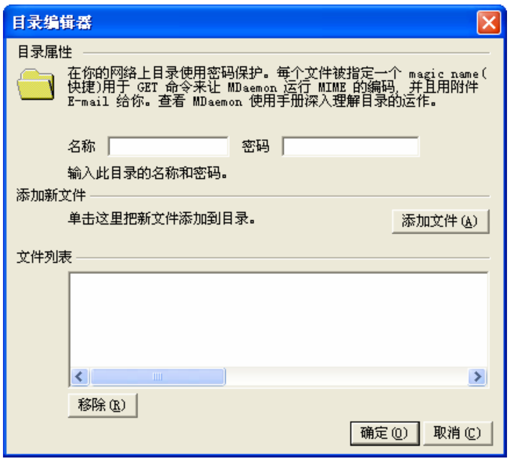
MDaemon ® 中文版

目录

使用**MDaemon**编录功能

使用“**编录**”-“**新建编录**”…或者“**编录**”-“**编辑编录**”菜单选项打开编录编辑器创建或编辑文档编录。编录功能能使用户将文档传输到网络进行编码然后回传给用户，编录通过允许邮件管理者赋“魔法姓名”（简化操作）给磁盘上的文档来工作。魔法姓名就好象指向位于可存取 MD 的某个位置的特定文档的别名。一个用户则可以使用一个特殊类型的邮件信息来要求文档使用魔法姓名。该特殊邮件信息的格式在“**远程服务器控制**”选项中有详细描述（详见**邮件列表和编码控制**中的 GET 命令 P433）。

编录编辑器



编录属性

名称
使用此字段为文档编录键入名称

密码
使用此字段为文档编录输入密码。

注意

从 MDaemon v3 版本开始，所有的编录都不再需要密码。用户可以不用密码登陆任意目录。

详见：

邮件列表及编码控制- **P433**

添加新文件

添加文件
点击此按扭来添加文档至编录。在选择您希望添加的文档后，您将会被提示您希望为其起的“魔法姓名”。

文件列表

窗口显示所有文档

邮寄名单和目录控制见 **416** 页

文件列表
这个窗口显示所有文档及在指定编录里注册的“魔法姓名”。在窗口双击某个文件可将其移除编录。

删除
点击该按钮可以把选中的文件从*文件列表*中删除。

公共编录

公共编录不同于普通编录的管理。通常情况下，要输入配置给本编录的密码才能进入编录。而公共编录则不需要。凡知道文档魔法姓名的用户都能浏览公共编录中所罗列的文档。

第二十六章

MDaemon ® 中文版

域网关

MDaemon 可以作为网关，需要添加和设置域

通过点击主界面菜单栏上的“网关”-“新建网关”或“网关”-“编辑网关”可到达网关编辑器选项。此特性能为主机的多重域（multiple domains)提供一个受限却有益的二级支持。此特性也还能作为一个后备邮件服务器使用。当邮件送达一个 MDaemon 担当网关的范围时，它将从主邮件流中分离出来并发送至网关编辑器中特定的目录中。此外，附件也会被自动读取放置在特定附件目录中。所有邮件还会根据它特定 MBF 文档重新格式化。用此方法，您就可以设置尽可能多的域。

举例证明其有益性：

如果您希望部分控管的其它部门的域。您希望收集其邮件并将邮件放在一个目录内但不希望在您的服务器上保留他的帐户。如“company.com”。首先，在编辑器的域设置中的“域名”字段中键入“company.com”。然后，选择键入接收邮件和文件附件存储的磁盘目录。除非需要，您不用自动提取附件特性。最后，选择现存的 MBF 文档或安装新 MBF 文档。默认值 PFC-822 MBF 文档保证所有存储在“company.com”的邮件格式都为 RFC-822。当所有设置完成后，点击“应用”或“完成”。

既然“company.com”作为一个客户域已经建好了，无论信息来自哪里，MDaemon 都可以按照您指定的格式把域接收到的所有信息存储在指定的目录里。换句话说，这个域所有的邮件都集中在磁盘中唯一的目录里。用户可以创建一个目录，也可以为域创建一个登陆的 POP/IMAP 帐号。创建帐号的方法是直接在网关编辑器里的网关编辑器里的 POP/IMAP 里输入用户名和密码，然后点击 Create/Upade Account 按钮确认。域收到的来自于 MDaemon 的邮件经过它的帐号保存了下来。这些工作既可以由邮件客户机来完成，也可以由另一 MDaemon 程序来完成，它可以使用自己的 DomainPOP 的功能把邮件分配给用户（同我们上面提到的例子）。或者，您也可以使用 ESMTP ETRN 和 ATRN/AUTH 的控制器为用户收集和分发邮件，这种方法用 ESMTP 替换了 POP，DomainPOP，IMAP。

以上所有的工作都是基于广域网或局域网的基础上，类似于”company.com”的例子，任意一个域的设置都能容易的完成。如果域不在因特网上，如何为”company.com”提供邮件服务呢。有两个方法可以解决。第一种方法，先去因特网的官方注册一个域名，域的 IP 地址要与用来接收邮件的 MDaemon 的 IP 地址相同。另外一种办法是以主域名的别名注册。如果不这么做，即使把

“company.com”“隐藏”在主域地址中，信息仍然能发送。使用这种办法，MDaemon 作为网关，地址被创建，通过主域传送到域的用户。例如来说，假如一个外部因特网的用户想给”bob@company.com”发送邮件，这是一个由”mydomain.com”支持服务的域网关，那么发信人必须把它的邮件信息发送到”bob｛company.com｝@mydomain.com”.因为”mydomain.com”被 MDaemon 注册为主域名，这条消息才能被正确的发送。如果 MDaemon 接收到的信息包含了地址，它将覆盖”bob@company.com”并把信息发送到域所指定的磁盘目录里。当然最简单的办法还是注册域名，把它的 DNS 信息指定给作为网关或支持服务器的 MDaemon。

网关编辑器

网关编辑器包括以下对话框：

网关

此对话框包含您工作需要特殊域的域名，及到存储邮件文档附件的目录的路径。当 MDaemon 发送邮件至此范围的邮箱时，您还应设置一个 MBF 文档供使用。

ETRN

使用此对话框的控键来选择是否由 MDaemon 代表域来响应 ETRN 的要求。为增加安全性，此对话框还包含使 MDaemon 准许这些请求而配置特殊 IP 地址的控键，或者您可指定忽略的 IP 地址。

ATRN

如您希望当 MDaemon 担当邮件网关时由 MDaemon 应答 ATRN 命令，则使用此标识符上的控键。该标识符还包含控键能验证指定域的共享机密，能指定无论是什么 IP 地址，验证需求都被视为有效。

选项

在此对话框内，您可以指定一个主机，当邮件发送到该域的时候马上转发至该指定主机。还有控键可标明邮件副件是否为本地邮件。

POP/IMAP

本对话框可创建一个 POP 账号以访问域下的邮件。使用设定的姓名和密码，一个普通的邮件用户或其他 MDaemon 安装程序都能进入域的邮箱，收集邮件。

限额

此对话框用来为限定域所需的磁盘空间的大小和所邮件存储的最大数量。

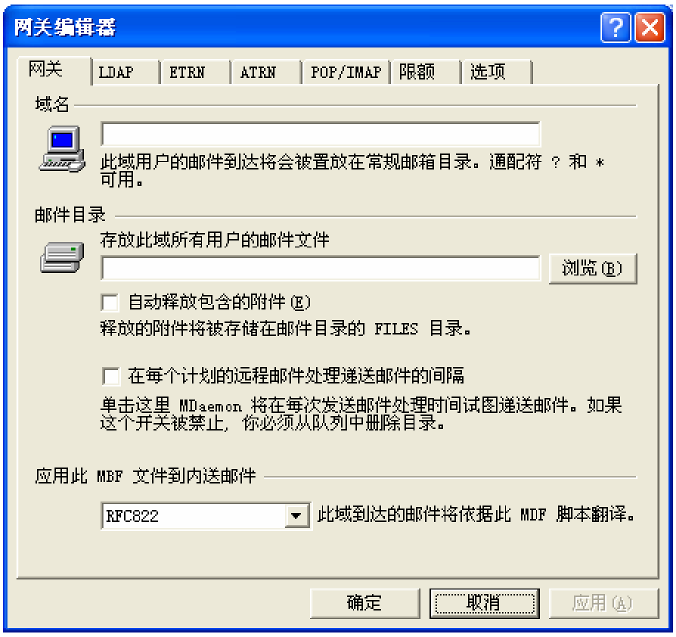
LDAP

如果网关的远程域维持着一个最新 LDAP 服务器和其邮箱，别名和邮件列表。您可使用本标识符来指定服务器然后校验接受地址。如接收地址无效，邮件将会被拒绝接受。通过这种方式，您可以避免接受所有那些无论有效与否都与网关域捆绑的邮件了。

自动网关创建

此对话框上的控键（网关-自动网关创建）能当其他来源试图发送域邮件给 MDaemon 时，使 MDaemon 为未知域提前自动创建一个域网关（P392），DNS 询问罗列 MDaemon 方位作为有效 MX 记录。

网关



域名
为您希望 MDaemon 担当邮件网关键入域名

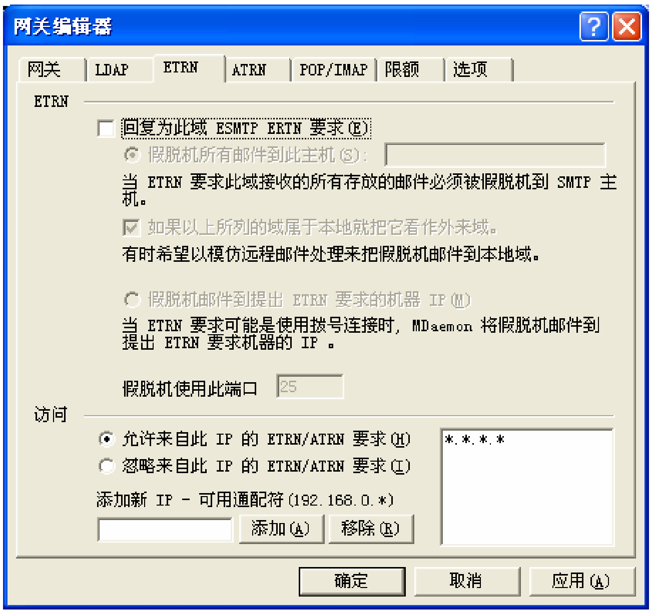
邮件目录

将该域所有用户的邮件文件置于这里
在您希望存储所收到的邮件处输入目录。

自动提取包含的附件
有些邮件系统要求附件需在邮件提交到邮件流之前被提取出来。方便起见，MDaemon 可自动提取所收到的 MIME 附件并将其放在\文档\域邮件目录下的子目录内。此目录只有在选择“自动提取”后方能使用。

按照每个预定的远程邮件处理时间间隔来投递邮件
通常来说，当 MD 收到确定为网关域之一的邮件时，它会将邮件存储直至连接到 MD 的域接收它为止。在有些情况下，您可能需要 MD 通过 SMTP 来发送邮件而不是等待域来接收。当此更能启用，MD 会在每一个远程邮件处理间隔发送域邮件。该网关的邮箱将暂时视为远程队列并执行发送命令。任何无法发送的邮件会留在网关的邮箱里直至域接收这些邮件或者稍后被成功发送，他们将不会被移动至远程队列或重试系统。
将该 MBF 文件应用于接收邮件
这里所特指的 MBF 文档会应用于所有发送到本域的邮件。这允许了任何可能的特殊格式化程序。

ETRN



ETRN

<u>回复为此域 ESMTP ETRN 要求</u>

打开此选项，MDaemon 响应对主机制定的 ESMTP ETRN 要求，表示域将以 MDaemon 作为邮件网关。ETRN 命令是一个 SMTP 的扩大，一个服务器为一个特殊域存储邮件，则可以开始假脱机邮件。当 MDaemon 从域接收到一个 ETRN 请求，它将立刻使用并发 STMP 程序开始为发送假脱机存储邮件。请注意发布 ETRN 要求的 STMP 部分不会是接收任何存储邮件的。MDaemon 会使用并发独立的 STMP 命令来发送为域所存储的任何邮件。这保存了邮件的信封，也更加安全可靠。同时注意，MDaemon 假脱机任何存储邮件至的主机可能不会立刻开始接收这些邮件。ETRN 只能保证所有存储的邮件为发送“假脱机”。实际的发送过程是服从于其他管理者设置的限制，也可能在输出邮件队列等待狭义次远程邮件处理计划的执行。由于上述种种限制，我们建议使用（ODMR）个其 ATRN 命令而不是 ERTN。不是所有的用户和服务器都支持此方法，因此只有使用服务器的用户域可使用 MDaemon 完全支持客户和服务器端。

<u>假脱机所有发至该域名或 IP 的邮件</u>

当 ETRN 请求被接受或被准许，任何存储的邮件将会被发送到此主机和 IP 地址。接收器必须运行一个 SMTP 服务器来接收邮件。注意：当在此选项内指定一个域名后，MX 和 A 记录在发送过程中会依赖 DNS 结果被使用。如果您希望将邮件发送至一个特定主机，则指定一个 IP 地址代替域名，这会为发送要求一个 DNS 检查过程。

如果上类域是本地的，将其视为外来域。
如果域是本地但您希望假脱机邮件就好象是远程一样则激活此控键。

将所有邮件假脱机到发出 ***ETRN*** *请求机器的* ***IP***
选择此选项，MD 会应将所有存储邮件发送到 ETRN 要求的机器的 IP 地址。此要求的机器必须运行一个 SMTP 服务器来接受这些邮件。

假脱机邮件时使用该端口
当域内的邮件假脱机时，使用此控键指定一个端口。

IP 访问

允许来自 ***IP*** *的* ***ETRN/ATRN*** *要求*
选择本开关，MDaemon 将准许任何在相关地址列表内罗列的 IP 生成的 ETRN/ATRN 要求。

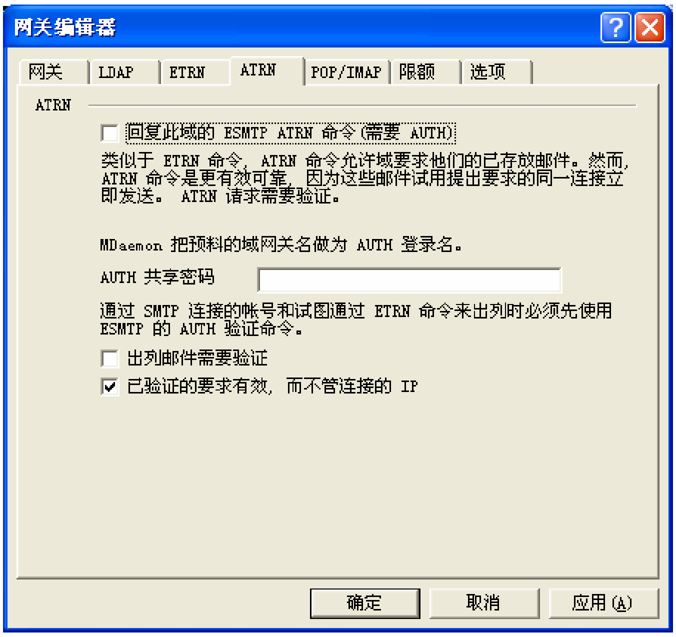
忽略来自 ***IP*** *的* ***ETRN/ATRN*** *要求*
选择本开关，MDaemon 将忽略任何在相关地址列表内罗列的 IP 生成的 ETRN/ATRN 要求。

添加新 ***IP***
在现有列表内添加一个新的 IP 只需简单在此文本框内输入 IP 并点击添加按纽。

删除
点击本按钮可删除在 IP 地址列出的被选条目。

提示
尽管屏幕显示中无任何地方可进入本控制条，但客户可控制 SMTP 信封 ID 使 MD 在假脱机域邮件时可以使用。其主要控制在以下文件中：
GATEWAYS.DAT
[[GatewayDomainName]
EtrnAs=address@domain.com

ATRN



ATRN

回复此域的 ESMTP ATRN 命令

如果希望回应域的 ESMTP ATRN 指令则激活本控制条，这样 MDaemon 将作为网关。ATRN 为当前 On-Demand Mail Relay(ODMR)的一个新的 ESMTP 指令，是当前邮件主机可获得的最好的延迟方法。它优于需要认证的 ETRN 和其他方法，在邮件被出列之前并不需要一个静态的 IP 地址。无需一个静态的 IP 地址，那是因为在 MDaemon 和用户的域之间的数据流被快速转换，并且这些信息在 despool 时无需新的连接（与 ETRN 不同，它在 ETRN 指令被发送后使用一个单独的连接）。如此可使用户的域使用一个动态（非静态）拨号帐号来搜集他们的信息，而无需使用 POP 或 DomainPOP 来把它们分配到用户中，因为原来的 SMTP envelope 是被禁止的。

AUTH 共享机密

键入验证过程中使用的客户域“共享机密”或者密码

注意

MD 担当网关的域必须使用域名为其登陆参数。

邮件队列需要验证

当你为域设置接收 ESMTP ETRN 请求，您可以使用此标识符控键来要求连接主机来先验证本身使用 ESMTP AUTH 命令。由于 ATRN 请求验证，此控键必须在 MD 响应 ATRN 需求前被启动。

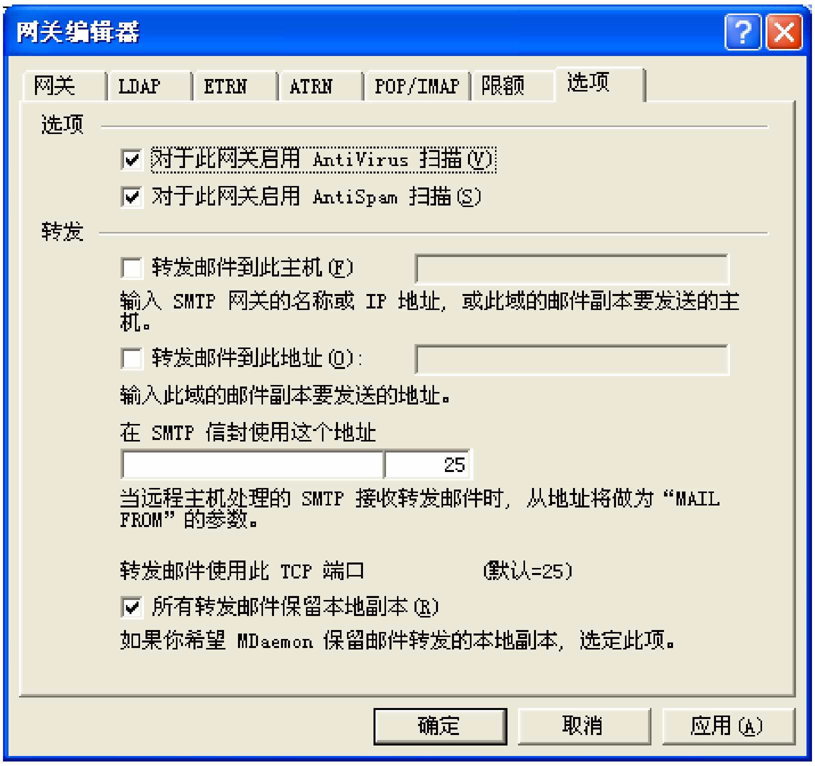
*已验证请求有效，而与连接 **IP** 无关*

如果您希望无论 IP 地址来自何方都准许验证请求，则启用此校验框。如果此控键没有启用，那么只有来自 ESMTP ETRN 标识符的 IP 存取选项中指定的 IP 地址的验证请求才会被准许。

作为该网关用户发送邮件时需要验证

如果您希望所有的声称来自域的邮件都请求验证，则点击此校验框。如果一封邮件假来自该域，那么它必须使用一个验证连接（或是连接到一个可信的 IP 地址）或被拒收。

选项



选项

启用该网关的防病毒扫描

如果您已经安装了 MDaemon 的反病毒插件且希望网关域的邮件都被扫描，请启用本选项。

启用该网关的反垃圾邮件扫描

如果您希望为网关域邮件应用垃圾邮件过滤设置，请点击本选项，不然，他们将会被排除在垃圾扫描过滤扫描之外。

转发

将邮件转发至此主机

有时，在邮件送达时，为一个域转发所有邮件的副本是十分有利的。如果您希望配置 MD 来完成此过程则输入名称或 SMTP 服务器的 IP 地址，让此域的接收邮件副本都发送到上述地址。

转发邮件至此地址

如果您希望将邮件转发至指定邮件地址，所有邮件都指向此用户域。

*在 **SMTP** 信封中使用这个地址*

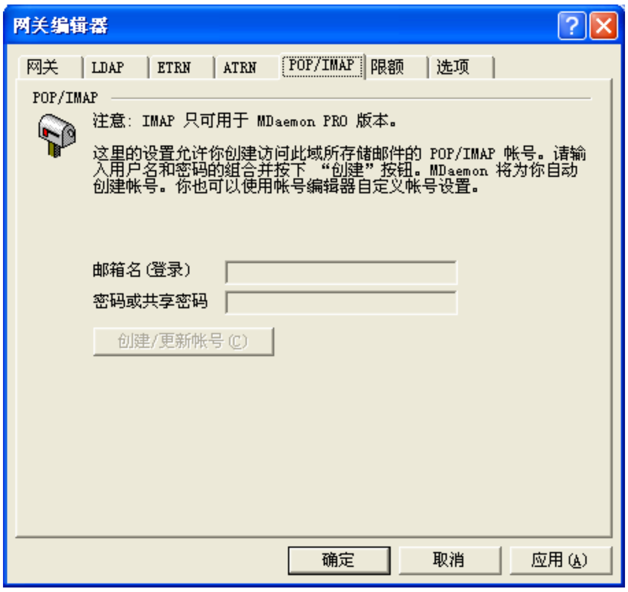
MDaemon 将在 SMTP“邮件来自于”处理过程中使用本地址。

*使用该 **TCP** 端口转发邮件*

通过 TCP 端口 MDaemon 可转发邮件

保留所有已转发邮件的本地副本
如果您希望 MDaemon 一旦邮件被转发则保留所有转发的邮件的本地副本，则选择本项。

POP/IMAP



早期 MDaemon 版本搜集邮件的方法是 DomainPOP(见英文 227 页)，MDaemon 除通过 DomainPOP 搜集邮件外，当以 MDaemon 为邮件网关时，亦可使用其它域的 DomainPOP 主机。换句话说，域的所有信息都可被搜集在服务器上的一个简单邮箱中。然后域将连接到用户并通过它自己的 MDaemon 来搜集信息，或通过正常的 POP 用户代替 MDaemon，尽管 DomainPOP 对它们并不能分解。在使用本对话框上时，将创建一个帐号使 MDaemon 能够使用保存在域网关中邮件。

由于 MDaemon Pro 支持 IMAP 邮件协议，当用户使用本协议来代替 POP 协议时，MDaemon Pro 创建的帐号也可被用户使用。

邮箱名（登陆）
使用用户的域进入 POP 用户名，可访问保存在邮件中信息。

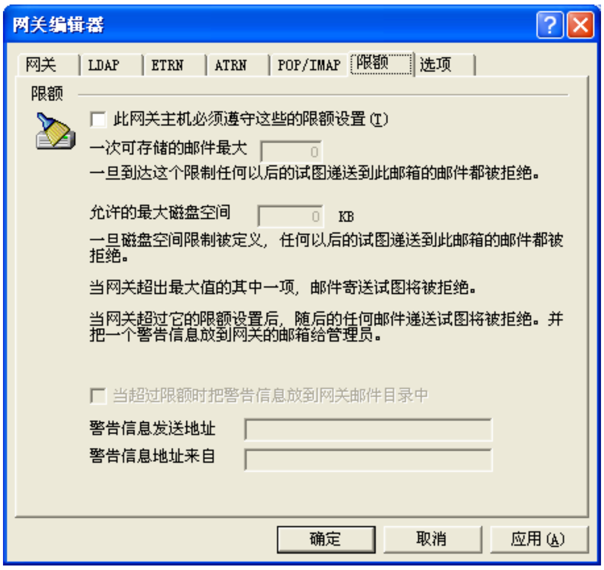
密码或共享机密
使用用户的域进入密码或共享安全，可访问保存在邮件中信息。

创建/更新帐号
点击进入，可创建或更新已经存在的邮箱名称和密码。

注意

用户可使用帐号编辑器来完全编辑（甚至删除）帐号。在删除帐号时需特别注意，因为这样将删除帐号里的邮件和文件路径－在网关中使用的亦会删除。

限额



限额选项

<u>此网关主机必须遵守这些的限额设置</u>

本条可定义域使用的最大信息数量及最大磁盘空间（按千字节计算），包括文件路径下的解码文件的附件。

<u>当超过限额时把警告信息放到网关邮件目录中</u>

使用本控制条，当发送到域的邮件超过最大信息数量及最大磁盘空间，则警示信息将被转发到指示的地址。

<u>警示信息发送地址</u>

定义超过配置的警示信息发送的地址。

<u>警示信息地址来自</u>

定义超过配置的警示信息发送到来源地址。

LDAP

一般的问题时域网关或备份服务器并不总是确定接受信息是否是有效的。如，一条发到 frank@example.com 的信息进入 example.com 的备份服务器，则备份服务器无法识别是否这是来自真正的邮箱、匿名或在 example.com 对于“frank”的邮件列表。因此备份服务器无法进行选择只能接收所有的信息。MDaemon 可以提供一种方法来甄别这些地址并解决这个问题。在远程域的 MDaemon 可设置保存 LDAP 服务器上的日期及所有邮箱、匿名和邮件列表（见英文 109 页）。如此，则用户可通过备份服务器上域网关编辑器中的甄别选项来定义 LDAP 服务器上的保存信息。现在，当发送到 example.com 一条信息，备份服务器将寻找 LDAP 服务器上的接收地址，找出是否为有效地，如果为非法的，这条信息将被拒绝。

LDAP 选项

使用 LDAP 服务确认帐号

点击 check box，激活远程地址鉴别。对于任何远程域，进入 LDAP 服务器的信息需确定接受者是否为有效的，如果为非法的，这条信息将被拒绝。

主机名或 IP

进入域的 LDAP 服务器的主机名称或 IP。MDaemon 将连接到 LDAP 服务器以鉴别域网关的地址信息。

注意

尽管可使用 LDAP 服务器，但推荐使用 Alt-N Technologies 的 LDAP 服务器的最新版本，LDaemon 2.1，因为其拥有统一的构架并容易设置。用户可从 ww.altn.com 上获得 LDaemon 的免费版本。

端口

定义域的 LDAP 服务器监控的端口。MDaemon 将通过这些端口来鉴别帐号信息。

测试
点击检查按钮，用户可设置远程地址鉴别。MDaemon 将简单的连接到指定的 LDAP 服务器并鉴别这些回应的特定信息。

邦定密码
这个密码可进入域的 LDAP 服务器，连同认证的 Bind DN 值。

对象类
定义每一个使用 MDaemon user LDAP 地址本登陆的用户级别。每次登陆包括用户级别 ＝ 赋值

邦定识别名
进入 DN 帐号，可使 administrative 访问域下的 LDAP 服务器，从而使 MDaemon 认证网关的地址信息。这就是 DN 认证的 bind 操作。

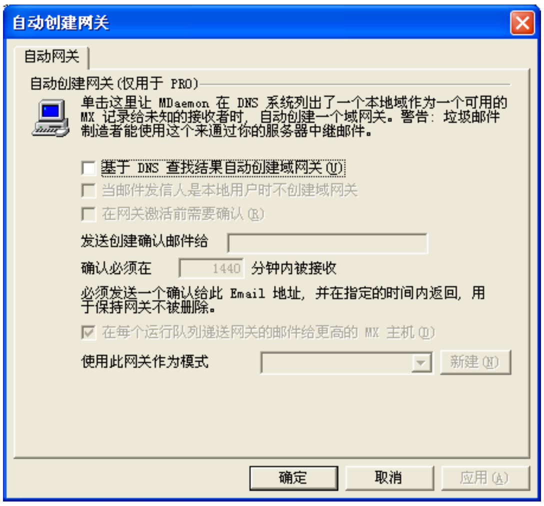
基底项目识别名
这是一个基础登陆（根 DN），使所有域网关下的地址信息拥有远程鉴别。

*属性包含 **Email** 地址（用逗号隔开）*
当使用 LDAP 服务器来鉴别域网关邮件接收时，可通过文本框来定义多重邮件分配。这种情况在某些时候是必要的，但 LDAP 服务器包含一个分配的保存邮件的地址和一个不同的分配保存匿名的地址，用逗号来区分不同的分配。

对LDAP验证队列使用多重配置
你能为你的网关域指定多重LDAP配置。为了指定额外的LDAP参数集，正常设置你的首个集合，然后使用记事本手动编辑GATEWAYS.DAT文件。

您的新的参数集应该用如下的格式创建：
```
LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
LDAPRootDN1=<root DN>
LDAPObjectClass1=MDaemonContact
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```
对于每个新的参数集，给每个参数名称中的数字增加1。例如，在如上的例子中，每个参数名都以“1”结尾。要创建另一个参数集，每个参数名将以“2”结尾。在又一个集合中，每个参数名将以“3”结尾，以此类推。当LDAP查询发生时，MDaemon将执行多重LDAP查询依次发现匹配。如果发现错误或发现匹配，不会进行进一步的检查。

自动创建网关



自动创建网关（仅适用于 **PRO**）

通过设置 MDaemon，本控制条可对于一个前所未知的域创建一个域网关（见英文 376 页），当另一个源试图发送域下的信息到 MDaemon，DNS 质疑的列在 MDaemon 的地段作为有效的 MX 记录。

例如：
激活自动网关创建，如果 MDaemon 的基本域 IP 地址为 1.2.3.4，经 SMTP 发送一条信息到一个未知的域 example.com，MDaemon 将运行 MX 和 A-record 来询问 example.com，检查 1.2.3.4 是否为已知的邮件传递主机。如果 DNS 询问的结果表明，对于 example.com，MDaemon 的 IP 地址为一个有效的 MX 主机，则 MDaemon 将自动创建一个新的域网关来接收它的邮件。example.com 的信息将被保存到指定的目录下，如果用户选择，则在每一个远程邮件处理间隙，汇集到高级的 MX 主机。这种特点使之成为一个备份服务器，对于另一个域来说，通过已使用的 IP 替换 MX 主机来简单设置 DNS 系统。

为保证这种特点，设置 MDaemon，发送一条确认要求到用户选择的邮件地址。当 MDaemon 等待确认的回复时，域下的信息将被接受并保存但不发送。回复确认要求，包括时间，当制定或自动创建网关后，这些将被删除，所有保存的也将删除。如果在时间过期前受到确认信息，则所有保存信息将被自动发送。

注意
目前一些恶意攻击者或"垃圾邮件制造者"试图利用此项功能来设置他们的 DNS 服务器查找出用户 MDaemon 的 IP 地址，作为他们的 MX 主机之一。因此自动创建网关功能在使用时需特别注意。为避免可能被恶意利用，推荐尽量使用发送创建确认信息功能。

<u>基于 DNS 查找结果自动创建域网关</u>
点击控制条，根据 DNS 查询结果，自动创建域网关

当邮件发信人是本地用户时不创建域网关
如果当信息来源为当地用户时，用户不希望自动创建网关，则点击本控制条。

在网关激活前需要确认
点击控制条，MDaemon 将发送确认信息到用户邮箱地址，确定是否自动创建网关，MDaemon 会持续接受来自域的询问信息直到收到确认为止。

发送创建确认邮件给
在文本框中列出希望发送确认信息的接收地址.

*确认必须在 **xx** 分钟内被接受*
在控制条内指定时间，则 MDaemon 将等待确认信息的回应。如果超过限定时间，域网关将停止追问。

*在每个队列递送网关的邮件给更高的 **MX** 主机*。
在每次远程队列处理时，MDaemon 将发送网关邮件到更高的 MX 主机。

使用此网关作为模式
从下载列表中选择域网关，MDaemon 将通过模板设置自动创建网关。

新建
点击新建按钮，将打开网关编辑器，创建一个新的域网关。

第二十七章

MDaemon ® 中文版

队列与统计管理

使用 MDaemon 的队列与统计管理

直接点击菜单队列→队列与统计管理…可以应用 MDaemon’s 队列与统计管理（MDStats）功能。MDStata 是一个由四个页标签（选项卡）组成的对话窗口。每一个页标签都有着特定的用途，应用起来非常简便。

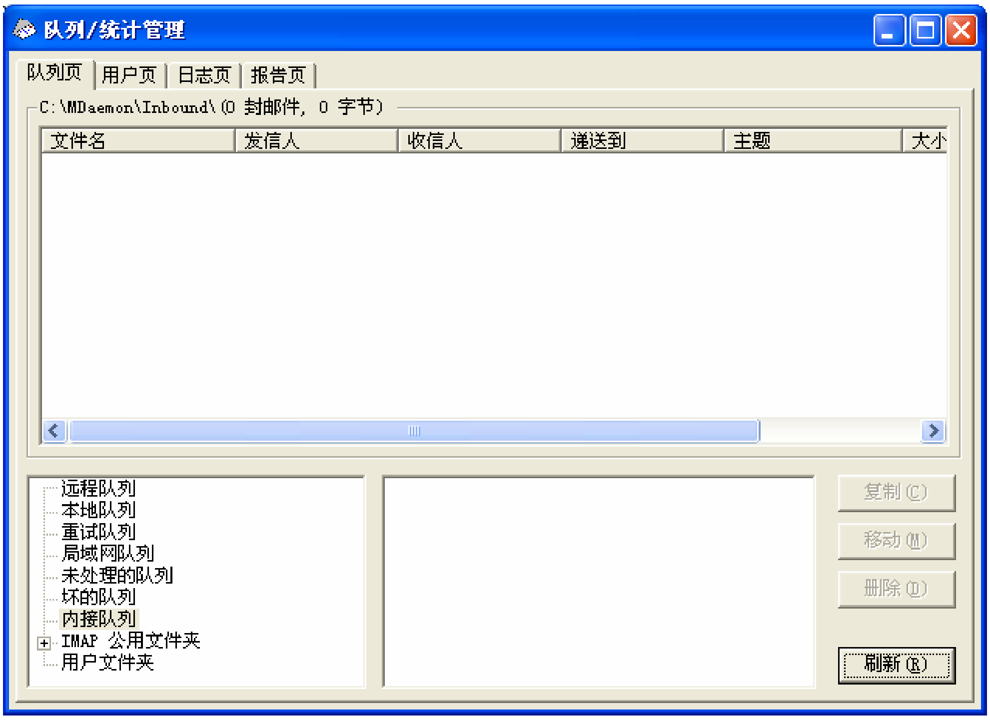
队列页面
默认项是队列管理。利用这个页标签用户可以很容易的对 MDadmon 的标准邮件队列和用户帐号的邮箱文件夹进行管理。只需要点击一个队列或指定的任一个用户，该队列中或用户文件夹中所包含的所有邮件以及每条邮件各自相关的重要信息显示出来：发信者，接收者，实际接受者，邮件主题，大小以及保存的时间。除此以外，在文件夹之间可以很容易的复制移动和完全删除。

用户页面
这个页标签罗列了 MDaemon 的所有用户。列表里包含了用户的全名，邮箱名称，邮箱中邮件的数量，账号占据磁盘空间的容量，以及用户最近一次访问邮箱的时间。这个列表可以以文本的形式存储，也可以以逗号分隔符数据格式存储以供数据库使用。

日志页面
在这个选项卡里，用户可以在一个简单的列表形式里查看 MDaemon 的日志文件。由于能概括日志文件的日志参数因此能快速的浏览 MDaemone 的邮件处理的历史信息。根据信息的类型，以列表的形式概括起来，这些类型包括（POP 接收、DomainPOP、RFC822 形式等等），Mdaemon 在处理邮件时连接到的主机，发送者，接收者，邮件的大小，处理邮件的时间以及处理邮件是否成功。如果用户想要查看某条信息的双击想要的条目就可以浏览列表中任意条目的相关日志部分的信息。信息处理完后，日志会显示出来。日志页里展示的所有日志都可以以文本的形式存储，也可以以逗号分隔符数据格式存储以供数据库使用

报告页面
“报告页”是最后一个页标签。利用这个选项卡，用户可以生成一个清晰明白的可读型的文本报告。这个报告包含了 MDaemon 的所有配置信息。因为 MDaemon 里有很多的设置和配置信息，在改变配置信息或者这些配置信息可能出现问题需要修改时，通过报告页可以提高速度。而且，这个报告是文本可编辑的形式显示的，所以在存盘前可以很容易地对报告所包含的信息进行复制/粘贴（使用右键弹出快捷菜单），或者增加符号和其它信息。

队列页



队列页列表

当从队列管理区域里选出一个队列或者从用户列表盒中选出一个用户，则被选中的队列里所有的信息文件都在这个页标签的主列表盒里显示出来。这个列表里包含了每个文信息的文件名，发送者，接收者，发送的报头，信息的主题，大小，以及在当前位置保存的期限（以日期和时间的形式显示）

在上面这个列表盒里，显示出了文件所在目录的绝对路径，信息的数量和目录的大小。

客户在列表里选中想要的信息，然后点击下面相关的按钮可以对选中的一个或多个信息进行复制、移动或者删除。

队列页列表盒里的文件内容都可以进行编辑。只要双击想要编辑的文件（或者右键快捷菜单中的"edit"按钮），MDStats 就可以打开 windows 的记事本对文件进行编辑。

注意

如果你想打开的是编辑器而不是默认的记事本，你必须在\MDaemon\app\diredtory\路径下编辑"mdstats.ini"文件。把原先的"editor=key located under the [queueoptions] section heading"改为"editor=youreditor.exe"(没有引用)。如果在你当前的目录里没有 exe 文件，你就必须把文件的路径作为文件

名的一部分。

用户可以用水平滚动条或垂直滚动条来定位列表也可以在列表盒的任意位置用方向指示键寻找想要的对象。你可以对从 queue page 列表盒里任意选取的列所包含的信息进行分类。对某列点击一次对该列进行升序排列（a-z,1-2），点击两次则对该列进行降序排列（z-a,2-1）。
把鼠标放在栏头上，拖动栏到想要的宽度，栏的大小可以被重新调整。

选择文件

选中某个文件	直接点击想要的文件
选择连续的文件	先选中文件列表中相邻文件的第一个文件，然后按住 shift 键，同时用鼠标选中相邻文件中的最后一个文件。 或者，用户可以再按住 shift 键的同时，用上下左右方向键、Home、End、Page up 和 page down 键选择相邻的文件
选择不连续的文件	按住 ctrl 键的同时，用鼠标在文件列表里点击想要的文件

信息队列
点击坐下方的窗体，队列页列表盒里将把指定的队列中包含的所有文件显示出来。如果用户点击用户文件夹选项，在用户列表盒里信息队列的右边将显示出 MDaemon 的所有用户列表。

用户列表框
当点击信息队列（左下方的窗体）中用户文件夹选项时，在用户列表盒中将显示出所有的 MDaemon 的用户。点击某个用户名将显示出所有包含在用户邮箱文件加的邮件信息列表。

刷新
由于信息是经常发送和接收的，MDaemon 是活跃的，所以信息队列也是动态变化的。用户应当有规律的点击这个按钮来刷新显示的文件列表。

注意
用户可以通过自己编辑 MDstats.ini 文件实现列表的自动更新。这个操作很容易，只要打开 MDaemon 的 app 目录下的 MDstats.ini 文件，在[QueueOption]标题下面给 autorefresh 赋具体的数值，来表示两次更新之间的时间间隔。如果赋“0”值表示你不想让列表自动更新。例如：Autorefresh=15（列表每 15 秒自动更新一次）。

复制
点击这个按钮就可以把选中的一个或多个文件复制到另外一个队列或用户的邮箱文件夹中。点击这个按钮后，复制邮件的对话窗口就会打开，在这个窗口里用户可以为被选中的需要复制的文件确定目标地址。

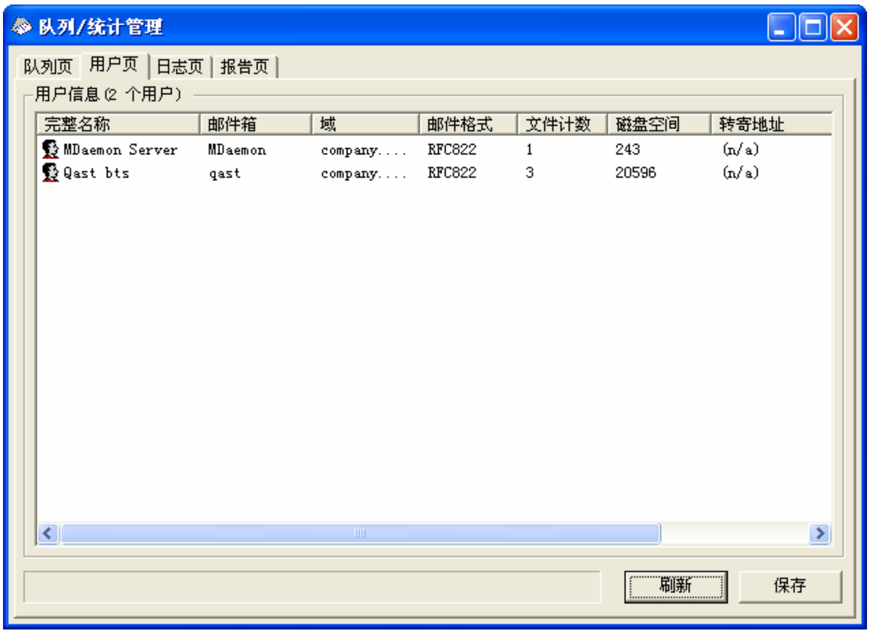
移动
点击这个按钮就可以把选中的一个或多个文件移动到另外一个队列或用户的邮箱文件夹中。点击这个按钮后，移动邮件的对话窗口就会打开，在这个窗口里用户可以为被选中的需要移动的文件确定目标地址。

注意
被复制或移动的文件一般很少保留原文件名。为了避免队列里同名的文件被覆盖，MDaemon 一般是基于目标文件夹中 HIWATER.MRK 文件来给第二个目标文件命名。

删除
点击这个按钮就可以把在 Queue Status List Box 中选中的一个或多个文件删除。用户在点击这个按钮后，会弹出一个对话框查询用户是否确认删除被选中的文件。

注意
因为信息处在不停的传递中，邮件列表是动态变化的，所以用户会认为在进行复制、移动、删除等操作时，MDaemon 会不停的提示用户以上的操作无法完成。如果用户对文件进行操作前，MDaemon 已经把该文件移走了，则用户会收到上面的提示。一般来说，用户应当先对文件列表进行刷新，对列表盒里显示的更新了的文件进行操作。
您也可以通过编辑 MDstats.ini 文件来防止信息在被操作的过程中被移出队列。这个操作也很简便，打开 MDaemon 的 app 目录中的 MDstats.ini 文件，把 [QueueOption]下的"LockOnEdit=No"改为"LockOnEdit=Yes".这样，在用户在对信息操作完成之前，LCK 文件可以防止这些信息被移出对列。

用户页



用户信息

如果选中用户页标签，则 MDStats 能够迅速的把 MDmemon 的所有帐号信息导入用户信息列表里。这个列表包含了每个用户的全名、邮箱名、帐号所属的域、信息的数量、邮件的格式、帐号所占磁盘空间的容量（字节）、转发地址和最后一次访问邮件的时间。如果列表中的信息不断的变化，点击刷新键可以很容易的更新。

用户可以用水平滚动条或垂直滚动条来定位列表，也可以在列表盒的任意位置用方向指示键寻找想要的对象。您可以对从用户信息列表盒里任意选取的列所包含的信息进行分类。对某列点击一次对该列进行升序排列（a-z），点击两次则对该列进行降序排列（z-a）。

把鼠标放在栏头上，拖动栏到想要的宽度，栏的大小可以被重新调整。双击某一条，MDStats 自动切换到队列页 ,邮箱文件夹里的内容会显示出来。

注意

缺省情况下，列表里显示的是消息的数量而不是文件的数量，消息所占磁盘空间的容量而不是目录里所有文件的容量。这个配额信息是由 MDaemonh 规定的。当然，MDStats 也可以显示文件的数量和目录中所有文件占有的磁盘空间容量。只要打开 MDaemon 中 app 目录里的 MDstats.ini 文件，把[QueueOption]下的

ShowQuota=Yes 项改为 ShowQuota=No 即可。

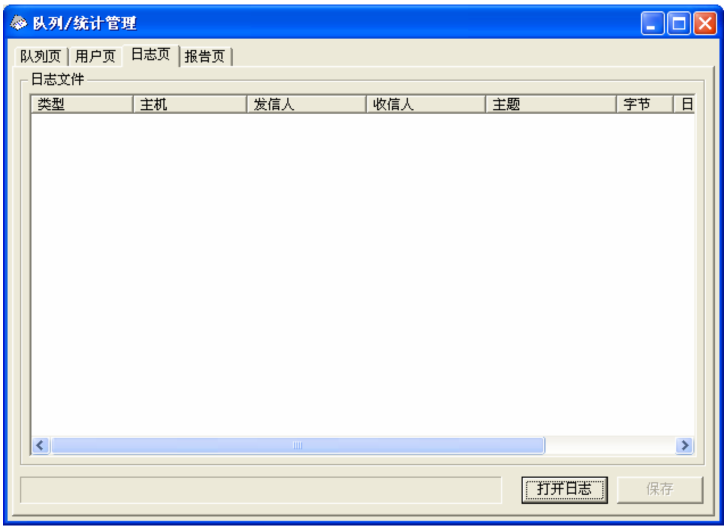
警告
MDStats 通过用户文件夹中的"hiwater.mrk"文件来确定该用户的一些信息。你要避免删除该文件，否则，MDStats 无法从 user list information 列表里获取相关的信息。

刷新
诸如邮箱里的消息的数量、帐号所用磁盘空间的容量这些用户信息也是常常变化的。为了确保这些信息的正确性，用户应当点击该按钮随时刷新 user information 列表盒中的信息。

进度指示
有时用户信息的列表可能会很大，在用户信息的列表盒下面有一个进程指示条。当 MDStats 加载大的文件时，指示条会显示程序运行的进度。

保存
用户信息中的信息可以以逗号作为分隔符的数据库形式保存，也可以直接点击 savejian 以 ASCII 形式的文本文件保存。在 windows 的保存对话框中，选择文件名和保存路径后，MDStats 将会询问用户是以数据库的形式保存还是以简单的文本文件形式保存。

日志页



用户点击打开日志按钮，在日志报告列表盒中显示出 MDaemon 所有详细的日志文件。MDaemon 对邮件操作前不必非要进行筛选，所以 MDaemon 日志文件里有时可能包含了大量历史纪录，日志报告可以为用户提供快捷简便的方法去浏览这些对邮件进行操作的历史记录。这些信息列表盒中展示日志文件时，MDStats 把日志文件分解成一个简单形式的内容：消息的类型（POP Inbound，DomainPOP，RFC822 等等），操作中连接到 MDaemon 的主机，发送者，接收者，消息的大小，处理每条消息的时间和操作是否成功。

用户可以双击想指定的条目了解关于该条目的详细地日志。日志会显示出消息是在哪个位置被操作的。通过使用右键弹出快捷菜单，你也把这些详细的日志复制/粘贴到文本编辑器中，按照用户的需要进行编辑并存盘。

用户可以用水平滚动条或垂直滚动条来定位列表也可以在列表盒的任意位置用方向指示键寻找想要的对象。把鼠标放在栏头上，拖动栏到想要的宽度，栏的大小可以被重新调整。

注意

通过点击 MDaemon 中的“设置→日志…”菜单项，用记录详细的邮件连接选项可以编辑日志页中的日志文件。但是我们一般建议用户最好选择记录详细的邮件连接选项。因为应用记录摘要的邮件连接，您会发现报告里显示的信息非常少。报告页本身可以把详细的日志精炼成 MDaemon 操作活动的概要，如果有需要，只要双击某个条目就可以浏览某个操作的详细信息，没有必要在让 MDaemon 生

成一个日志文件。

打开日志

点击该按钮可以打开 windows open 的对话框，在这个对话框中用户可以选择想要浏览的日志文件。日志文件将在列表盒中显示，MDStats 会给出搜索到日志文件的路径供用户选择。

显示日志后，会打开一个消息盒，包含着被指定的日志的概要。当一份日志报告已文本文件的形式保存时，这份日志概要会附加在后面。

进度指示

由于日志文件可能会很大，the log report 的列表盒下面有一个进程指示条。当 MDStats 加载大的文件时，指示条会显示程序运行的进度。

保存

日志报告中的信息可以以逗号作为分隔符的数据库形式保存，也可以直接点击保存键以 ASCII 形式的文本文件保存。在 windows 的保存对话框中，选择文件名和保存路径后，MDStats 将会询问用户是以数据库的形式保存还是以简单的文本文件形式保存。

报告页

报告

当点击 report page 选项卡时，MDStats 会生成一份容易读取的文本形式的报告，这份报告罗列出了 MDaemon 里全面详细的设置信息。这个功能大大缩减了管理者对各种配置信息核查的时间，从而能够快捷的解决配置方面可能出现的问题。用户可以滚动条或者方向键定位报告，报告是以文本的形式显示的，这样用户就可以在保存报告前插入符号或者额外的信息。并且，用户可以点击鼠标右键利用弹出的快捷菜单对报告进行剪切、复制、粘贴操作。

刷新

点击该按钮可以更新报告中显示的 MDaemon 的各种配置信息。

进度指示

与 MDStats 里的其它键一样，the repor page 也有一个进程指示条。当加载大的文件或者保存文件时，指示条会显示程序运行的进度。

保存

保存当前显示的报告。点击该按钮后，会弹出一个保存的对话框，在这个对话框中用户可以指定文件名和想要保存的位置。

定制队列与统计管理

下表是位于 MDaemon 的 app 目录下的 MDstats.ini 文件，罗列出了设置方面的信息，这些信息可以修改 MDstats.ini 文件

MDstats.ini File

[MDaemon]	
AppDir=C:\mdaemon\app\	Location of MDaemon’s \app\ directory.
[QueueOptions]	
Editor=NOTEPAD.EXE	Editor to use when a message is double-clicked, or when a message is right-clicked and then Edit is selected.
LockOnEdit=No	Whether or not to create a LCK file when editing a message. This will prevent a message from being moved out of the queue while it is being edited.
AutoRefresh=Yes	Time (in seconds) between auto refreshes of the message listing. 0 means no auto refresh.
ShowDirectories=Yes	Show subdirectories of the queues in the list box in addition to the messages. Directories will appear as <DirectoryName>.
[UserOptions]	
ShowQuota=Yes	Determines whether the user listing displays quota information (message count and disk space just like MDaemon calculates it) or file information (number of files and total disk space).
[LogOptions]	
ShowUnknown=Yes	Show sessions that MDStats couldn’t determine if they were inbound or outbound, SMTP or POP.
ShowSmtpInbound=Yes	Show SMTP inbound sessions.
ShowPopInbound=Yes	Show POP inbound sessions (mail checks).
ShowSmtpOutbound=Yes	Show SMTP outbound sessions.
ShowPopOutbound=Yes	Show POP outbound sessions (MultiPOP, DomainPOP).
ShowRFC822=Yes	Show RFC822 local mail deliveries.
ShowSmtpHelo=Yes	For SMTP inbound sessions, show HELO domain in the Host column.
IgnoreEmptyPop=Yes	Ignore mail checks when no mail was deliverd.
ShowImap=Yes	Shows IMAP Sessions.
[Remap]	Drive letter remapping; for running MDStats from a different machine than the one MDaemon is on. C:=\\server\c When reading from MDaemon.ini, replace “C:” with “\\server\c”.
[Special]	

OnlyOneInstance=No	Allow only one instance of MDStats to run. Attempting to open it again will activate the instance that is already running. This option can be set on the GUI tab of Miscellaneous Options by enabling or disabling the control: "Restrict MDStats GUI to a single instance only".

MDStats Command Line Parameters

Note: All command line parameters are not case sensitive.

Number 1 through 8	Display a specified queue in the Queue Page. 1 = Remote Queue 2 = Local Queue 3 = Retry Queue 4 = LAN Queue 5 = RAW Queue 6 = Bad Queue 7 = SmtpIn Queue 8 = Save Queue
/L[N] [InputFile] [OutputFile]	Produce a log file report. Specifying an 'N' after the 'L' means do not save as a comma delimited file.
/A	If producing a log file report, append new information to the output file rather than overwriting it.

第二十八章

MDaemon ® 中文版

MDaemon 的附加功能

MDaemon 的附加特性，功能和统计

带宽限制

新的带宽限制功能使您能管理和监控 MDaemon 所使用的带宽。您可以控制某会话或服务器的比例---在每一个域的基础上， MDaemon 的每一个主要服务器可规定不同的比例，包括初级、次级和域门。您也可以在一个下拉框中通过选择“本地通信量”从而限制在本地连接上。这将允许您创建特殊的带宽设置，从而在连接到或被本地 IP 地址或域名连接时启动。筛选功能的设置是为了使您能设置您自己的本地 IP 地址和域名清单。

带宽限制可在每个会话或每个服务器的基础上使用。当在使用每个会话模式时，每个会话将分别根据设置的比例节流。因此，同时产生的同一服务器类型的多个会话可能会超出一个服务的、设置的值。如果在每个服务器的基础上设置带宽限制，MDaemon 将监控同一服务器类型的所有会话的结合使用并对每一个会话分配同样的带宽。多个会话将共同平均使用设置的最大带宽。这将允许你对整个服务器进行设置。

当对一个域门设置带宽限制时，与普通的域有所不同。这是因为域门没有一个特定的 IP 地址与其连接。MDaemon 必须通过使用通过 RCPT 指令的值来决定一个本地的 SMTP 会话是否是在门的本地范围内。如果是，本地的 SMTP 会话的带宽限制将适用。因为 SMTP 的限制，即使多个收件人邮件的一个收件人被指定为一域门，那么整个会话将被节流。

带宽限制将以千字节每秒（KB/S）计算。“0”表示此会话或服务器没有速度限制，因此它将可以使用可利用的最大带宽量。例如，“10”将使 MDaemon 刻意对传输速度进行节流，即使其保持在或稍大于 10KB/S 的速度。

在一会话开始的突然运行可能使并将会超出限定的范围。节流将在会话过程中开始起作用并达到稳定。

带宽限制

带宽限制

把限制应用到每个基本服务（默认值是每个连接）

如果您想对每个服务器，而不是默认的每个会话节流带宽，请选择此项。当对每个服务器节流时，设置的服务器的带宽将平均分配给所有此服务器类型的现行会话。因此，例如，无论多少用户连接，同时连接的多个 IMAP 用户使用的带宽总量将不会超出设置的量。如果对每个会话节流，那么不会有一个 IMAP 会话超出设置量，但多个同时会话的总量可能会。

最大传输速度（KB/S）

从下拉列表框中选择您连接的最大速度，以千字节每秒（KB/S）为单位。

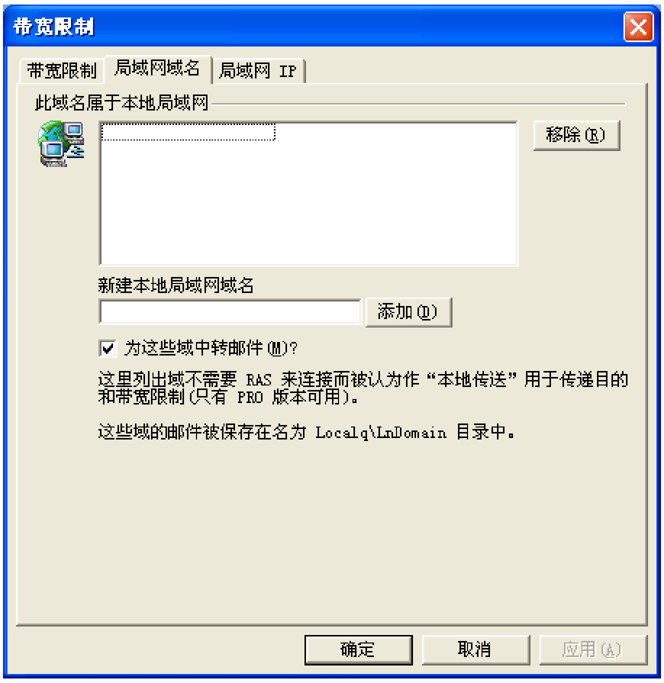
配置预设置

从下拉列表框中选择域，然后对选择的域调整不同服务器设置的带宽限制的选项。设置特定的某一个控制为“0”指没有带宽限制此服务器类型。在下拉列表框中，最下面列出的是本地通信量。对此选项设置带宽限制将决定对本地通信量的限制（即，会话和服务器出现在您的本地局域网上，而不是在外部局域网上）。局域网域和局域网 IP 标签在列举应为本地域和 IP 地址时使用。

[服务]带宽限制 – XX KB/S

从下拉列表框中选择了域后，调整控制从而对选择的域设置带宽限定。“0”设置即为此服务器类型没有带宽限定。将滑动条设置为“0”以外的任何数字即将指定的服务器的带宽限制为此数字的千字节每秒的最大带宽。

局域网域名



注意

此对话框与 RAS 拨号设置（见 223 页）中的同名对话框是相同的。在其中任意对话框中的变动将会显示在此两个对话框中。

此域名属于本地局域网

MDaemon 认为在此列出的域即为您的本地局域网中的一部分。因此，在节流标签中设置本地通信量将决定他们的带宽限制量。

新建本地局域网域名

在本地域单中添加一个新的域名，并点击“添加”键进行添加。

对这些域中转邮件

如果选择此功能，MDaemon 将对这些域传递信件。这将对这些域的通信量的发送和接收进行控制。

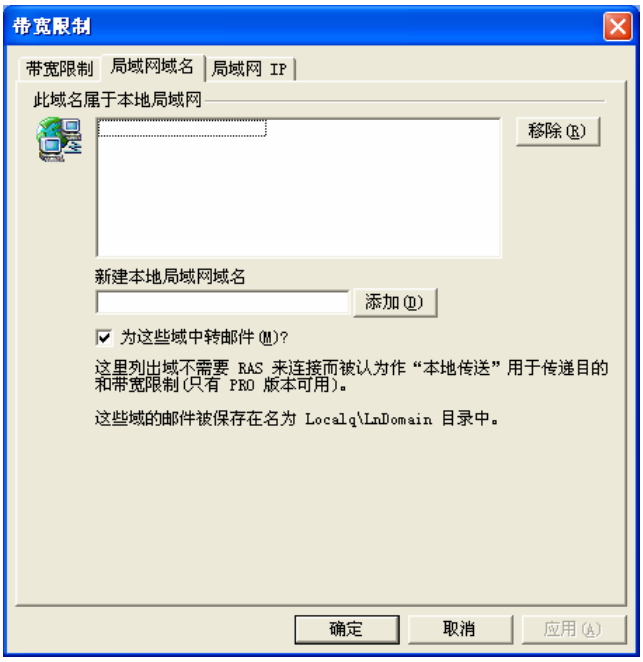
添加

点击此键在局域网域列表中添加一条目。

移除

点击此键将从局域网域列表中删除选择的条目。

局域网IP



注意

此对话框与 RAS 拨号设置（见 209 页）和安全设置（见 188 页）中的同名对话框是相同的。在其中任意对话框中的变动将会显示在此所有对话框中。

下列 **IP** 是我的本地局域网

此标签为原来在您的局域网中列出的 IP 地址。这些 IP 地址因此不要求 RAS 的连接，而且它们被以带宽限制为目的认为是本地通信量。另外，因为它们是本地地址，它们可能会被其它不同的保证安全和防止垃圾邮件的限制遗漏。

移除

从列表中选择一个 IP 地址，然后点击此键将其删除。您也可以双击一个 IP 地址从而删除它。

新的本地局域网 IP

在本地 IP 列表中输入一 IP 地址，然后点击“添加”键。通配符如 127.0.*.*是可以的。

添加

在新的本地局域网 IP 控制中加入新的 IP 地址，点击此键将其添加到列表中。

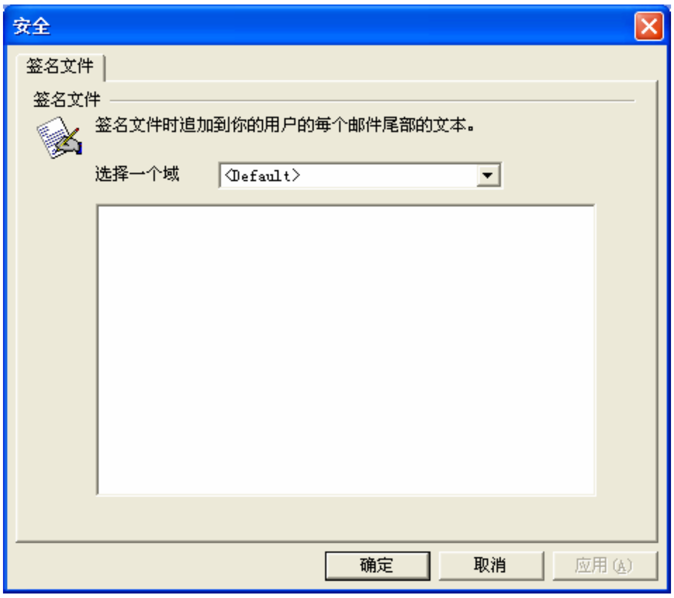
当处理邮件头时隐藏本地 IP

如果你想让 MDaemon 在它创建接收的报头时隐藏所有的 IP 地址，请点击此框。

…也隐藏这些局域网 IP

如果设置 MDaemon 隐藏本地 IP 地址，而你同时也想隐藏这些局域网 IP 地址，请点击此框。

签名文件



签名文件

本对话框可使您简单的设置默认的和每一个域的信件的签名文字。如果显示默认的签名文字，它将附加在从所有本地使用者发出的所有邮件中---除非某一使用者的具体域提供了另外的文字。如果找到具体的域文字，它将优先于默认的文字。

MDaemon的文字编辑器

MDaemon 服务器 v8 提供了一个文字编辑器，可通过选择文件→新建菜单打开。文字编辑器可为自动恢复和其它 MDaemon 功能快速创建数据文档，如 MBF 和 RAW 文档。

编辑MDaemon文件

MDaemon 文字编辑器也可用于编辑一系列 MDaemon 使用的现有文件。您能使用菜单选项打开这些文件：**文件→打开→[文件名]**。如果您想打开的文件没有列在**打开**菜单中，那么请点击**一般文件**选项。当您完成对文件的编辑时，请点击**文件→保存**或**另存为**。

打开选项中当前所列的所有文件如下所示：

- 最新版本发布信息

- 服务器使用政策
- 帮助信息
- 新用户欢迎语
- 项目信息
- 瞬间传递失败信息
- 永久传递失败信息
- 接收回传信息
- “无有效指令”信息
- “没有此用户”信息

- MX 隐藏数据库

- IP 隐藏数据库
- IP 保护数据库
- 无隐藏数据库
- 传递控制数据库
- 地址别名数据库
- 报头翻译数据库
- MIME 型定义数据库
- IP 筛选数据库
- 优先信件数据库

RAW邮件说明v3.1

MDaemon 服务器 v8 支持一个简单而强大的邮件信息格式，即 RAW 邮件。由于需要发展简易邮件客户而开发了此说明。RAW 系统的目的在于提供一个简单、标准的格式，而软件系统如 MDaemon 可以使用其创建很复杂的 RFC-822 适应信息。使用传递代理如 RAW 允许客户软件从服务器上卸下所有复杂的粘贴工作，而使信息变成 Internet 邮件标准。

RAW 邮件由一系列要求的和可选择的文字报头组成，还包括一个信息主要部分。大多数报头包括一个标记，随后是一个在＜＞符号中的值。每一个报头行以＜CRLF＞与字符结尾。所有的文字，报头和主体，为简单的 ASCII，并且包括在一个以 RAW 结尾的文件里。报头由一空白行与信息主要部分分开。报头*发件人*和*收件人*是必须注明的。

From ＜mailbox@host.com＞	此栏为发件人电子邮件地址。
To＜mailbox@host.com[,mailbox@host.com＞	此栏为收件人电子邮件地址。多个收件人之间用逗号隔开。
ReplyTo＜mailbox@host.com＞	可选择填写的、回复邮件发送到的电子邮件地址。
CC＜mailbox@host.com[,mailbox@host.com＞	可选择的复写抄送收件人列表。多个复写抄送收件人之间用逗号隔开。
Subject＜text＞	邮件的标题
Header＜Header: Value＞	你可以明确本邮件附有报头。

RAW v3.1支持的特别领域

加载附件和编码：
X-FLAG=ATTACH<FILEPATH,MRTHOD> (-X)

例如：X-FLAG=ATTACH <C:\utils\pkzip.exe,mime>-x

X-FLAG 具体化了“附加”值以及两个＜＞符号中的参数。第一个参数是一个完整的、应附加在邮件中的文件路径。第二个参数与第一个参数用逗号隔开，并在附加邮件时具体化了使用的编码。**MDaemon 服务器 v8** 支持此参数的两个值。MIME 方法指示服务器使用 Internet 标准的 Base64 方法的邮件编码。ASCII 方法指示服务器简单的把文件导入到邮件中。在一行结尾的可供选择的-X 参数指示服务器服务器在附加上文件后将其删去。

传递状态通知：
X=FLAG=CONFIRM-DELIVERY
当把一个包括此标记的 RAW 邮件转换成 RFC-822 邮件时，此行将变为“Return-Receipt-To：＜mailbox@host.com＞”。

在 **RFC-822** 邮件中加入具体的报头/值：

如果您想在 RFC-822 邮件中加入一个由 RAW 文件产生的报头/值，您将需要使用报头宏。例如，如果您想报头“Delivered-By:mail-machine@domain.com”加入到 RFC-822 邮件中，您需要在 RFC-822 邮件中加入“报头＜Delivered-By:mail-machine@domain.com＞”。请注意，“报头”宏要求领域和值。您可以在 RFC-822 邮件中添加无数个您需要的“报头”。

RFC-822 邮件例如：

1)
```
from <mdaemon@altn.com>
to <JohnSmith@somewhere.com>
Hello John!
```
2)
```
from <JohnSmith@nowhere.com>
to <President@Whitehouse.gov>
subject <Secret FBI Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\secret\files\dole.zip, MIME> -X
Here are all those files you asked for.
```

通过电子邮件远程控制服务器

MDaemon 服务器 v8 的很多功能都可以通过其电子邮件发送系统远程控制。例如，使用者可以遥控他们自己的账户，并可以通过向服务器发送电子邮件而改动或重新设置。MDaemon 在用户端保留一个其自己的账户。此账户可通过发邮件到 MDaemon@MDaemonsdomain.com 连接。发送到服务器的邮件储存在服务器邮件目录中。服务器定期浏览其收到的所有邮件并对邮件进行分类。

一些控制邮件要求服务器有一个有效的帐号，并由密码保护。使用者可通过密码进入帐号，同时所有的邮件都必须转入 MDaemon@mydomain.com。对于要求服务器要有有效的命令，邮件的主体必须包括使用者的 email 地址和密码，中间用逗号隔开（例如，Bill@maydomain.com, MyPassword）。命令添加在邮件主要部分中。一行只能由一个命令，但多个命令可添加在同一个邮件中。

帐号的访问和控制

如下列出了当前帐号拥有者进入帐号和控制帐号可使用的命令。所有的这些命令都要求在主题栏中填写“注册，密码”。包括在括号中的参数可选择填写。例如：“名称[地址]”可只填入“Lois”，或填入（Lois LLane@dailyplanet.com）.

COMMAND	PARMS	DESCRIPTION
ACCOUNT INFO	none	The status of the account passed in the subject line is mailed back to the originator. Ex: ACCOUNT INFO
PASSWORD	new password	The password of the account passed in the subject line will be changed to the one specified. Ex: PASSWORD kryptonite
MAILFORMAT	MBF file	The mailbox storage format of the account specified in subject line will be changed to the one specified. A listing of the available formats can be obtained via the MAIL FORMATS command (see General Email Controls section below).Ex: MAILBOX RFC-822
AUTODECODE	Y/N	Automatic decoding of incoming MIME attachments for the account specified in the subject line will be turned on or off. Y=on, N=off. Ex: AUTODECODE Y
BEGIN SIGNATURE	none	Begins recording of a new signature file to be appended to messages generated by the account passed in the subject line. Subsequent lines will be treated as the text of the signature file until the word END is encountered on a line by itself or the end of the control message is reached.**NOTE:** The signature file feature is only available for RAW format messages. RFC-822 mail that arrives at the server using SMTP or POP will not append the signature file. In these cases see your mail client’s documentation for information concerning signature files.
BEGIN AUTORESPONDER	none	Begins recording of a new autoresponder file. Subsequent lines will be treated as the text of the autoresponder until the word END is encountered on a line by itself or the end of the control message is reached. Ex: BEGIN AUTORESPONDER I’m on

		vacation right now. I'll get back to you ASAP. END To erase an active autoresponder, use the same command but without any response text. Ex: BEGIN AUTORESPONDER END
FORWARD TO	address	The forwarding address for the account passed in the subject line will be changed to [address] and mail forwarding will be activated for the account. Ex: FORWARD TO vacationing@myhost.com
UNFORWARD	none	Mail forwarding will be deactivated for the account specified in the subject line. Ex: UNFORWARD
MULTIPOP	on/off	MultiPOP will be enabled/disabled for the account specified in the subject line. Ex: MULTIPOP ON Ex: MULTIPOP OFF

邮件清单和分类控制

这些命令不要求服务器有帐号；因此，主题栏中不用包括任何具体的值。在括号中的参数可选择填写。例如：“名称[地址]”可只填入“Clark”，或“Clark CKent@dailyplanet.com”。命令参数必须包括“{}”或“()”。

COMMANDS	**PARMS**	**DESCRIPTIONS**
USERS	none	A listing of all user accounts which are not flagged to hide their information will be mailed back to the message originator. Ex: USERS
LIST	none	A listing of all non-concealed named lists (*Mailing Lists* that are configured to respond to LIST commands) along with the names and addresses of all members will be mailed back to the message originator. Ex: LIST [listname] Retrieves the membership of the list "LISTNAME" if it is configured to respond to the LIST command. Ex: LIST MDSUPP [listname (listpass)] This command retrieves the membership of the list "LISTNAME" even if it is configured to ignore the LIST command; as long as the list password is correct. Parentheses around the list password ARE required. Ex: LIST MDSUPP (THERIGHTPASSWORD)
SUBSCRIBE	listname [address] [{real name}] [(pass)]	The originator is added to the membership of the specified list provided that list exists and allows remote subscriptions. If an optional address is specified after the list name then that address is added to the list's membership rather than the address found in the FROM: field of the subscription message. A real name can be added for the subscriber by including it in braces (e.g. {Frank Thomas}. If the list's password follows this command

(parentheses around it are required) then the command will be honored even if this list’s subscribe function is switched off.

Ex: SUBSCRIBE mdsupp

Ex: SUBSCRIBE mdsupp me@mydomain.com {Frank Thomas}

Ex: SUBSCRIBE mdsupp you@yourdom.com (MDPASS)

UNSUBSCRIBE listname [address] [(pass)]

or

SIGNOFF

The originator is removed from the membership of the specified list provided that list exists and contains the originator as a current member. If an optional address is specified after the list’s name then that address is removed from the list’s membership rather than the address found in the FROM: field of the unsubscribe message. If the list’s password follows this command (parentheses around it are required) then the command will be honored even if this list’s unsubscribe function is switched off.

Ex: UNSUBSCRIBE MDSUPP (MDSPASS)

Ex: SIGNOFF MDSupportList me@mydomain.com

UPDATE listname old-address new-address {real name} (password)

Removes “old-address” from the list and replaces it with “new-address”. An optional real name and password value may be given.

Ex: UPDATE mdsupp@altn.com old@my.com new@my.com {Mr. M}

Ex: UPDATE mdsupp@altn.com old@my.com new@my.com (pass)

SUPPRESS listname address (password)

This command adds 'address' to the lists suppression file. The list's password must be provided and the list must already have a suppression file associated with it.

Ex: SUPPRESS list@mydomain.com

Ex: SUPPRESS me@mydomain.com (PASS)

UNSUPPRESS listname address (password)

This command removes 'address' from the lists suppression file. The list's password must be provided and the list must already have a suppression file associated with it.

Ex: UNSUPPRESS list@mydomain.com

Ex: UNSUPPRESS me@mydomain.com (PASS)

DIGEST listname [address] The sender is set to receive mail from the list in digest format. If an optional address is specified after the list name then that address is set to digest mode.

Ex: DIGEST MDSupportList

Ex: DIGEST mdsupp joe@mdaemon.com

NORMAL listname [address] The sender is set to receive mail from “list” in normal (non-digest) format. If an optional address is specifed after the list name then that address is set to receive in normal format instead of the sender.

Ex: NORMAL MDSupportList@mydomain.com

Ex: NORMAL mdsupp@mydomain.com joe@mdaemon.com

NOMAIL listname [address] This command sets 'address' to nomail mode. The account will enter a suspended state and will no longer receive list traffic. If no address is specified then the originator of the message will be used.

ex: NOMAIL list@mydomain.com me@mydomain.com

MAIL	listname [address]	This command returns 'address' to normal mode from nomail mode. If no address is specified then the originator of the message will be used. Ex: MAIL list@mydomain.com Ex: MAIL list@mydomain.com me@mydomain.com
REALNAME	listname [address] {real name}	This command sets the real name value for "address" who is a member of list "listname" to the given value. The real name must be enclosed in { and } characters. Ex: REALNAME mdsupp@altn.com {Frank Thomas}
GET	catalog magic-name (password)	Retrieves a file from the specified catalog, MIME encodes it in an email message, and sends that message to the originating account or to the one specified in a RESULTS TO directive. Ex: GET utils myutil (mypass) **NOTE: The special PUBLIC catalog doesn't require a catalog name or password in order to retrieve a file.**
DIR	catalog	Retrieves a directory of the files and magic names available through the catalog. Ex: DIR public.

通用邮件控制

COMMANDS	PARMS	DESCRIPTIONS
HELP	none	A copy of the help.dat is processed and mailed back to the message originator.
RESULTS TO	address	The results of subsequent instructions are redirected to the email address specified rather than to that of the message originator. Ex: RESULTS TO someone@somewhere.com LIST MDSUPP
STATUS	none	A status report on server operations and current conditions will be mailed back to the message originator. Since the information contained in this status report is considered private the subject of the requesting message must contain the an Administrator level user and password such as: Administrator, Password Ex: STATUS
MAIL FORMATS	none	A listing of all the supported mailbox formats will be mailed back to the originator. Ex: MAIL FORMATS
GET ADDRESS	none	MDaemon will send a message back to the originator which will contain the current machine name and IP address assigned to MDaemon's computer. This is useful when you want to find out the IP address assigned by your ISP when using a dynamic dial-up situation. Since the information contained in this message is considered private the subject of the requesting message must contain an Administrator level user and password such as: Administrator, Password Ex: GET ADDRESS

MDaemon和代理服务器

MDaemon 服务器 **v8** 被设计为通用的。因此，它可以和其它不同的网络设置和产品共同使用。MDaemon 机动性其与局域网代理服务器，如 WinGate，共同使用。为了设置 MDaemon 与任何代理服务器共同使用，您必须保证 port 设置（见 45 页）与代理服务器自己的设置不冲突。例如，SMTP 邮件通常发生于 port25。自从 IP 地址只能有一个 port25，两个服务器不能同时在一个机器上列出。在企图结合 MDaemon 和一个代理时，建议您允许 MDaemon 尽可能的对邮件撰写和传递进行控制。为此，代理中的 SMTP 和 POPport 应不得使用，从而 MDaemon 可独立控制邮件传递。

但是，您可以通过代理传递邮件，MDaemon 允许您设置用于发送和接收 SMTP/POP/IMAP 传输的 port。您需要设置这些 port 为无标准，从而通过代理服务器或防火墙过滤 SMTP/POP/IMAP 传输。

关于设置 MDaemon 与一代理服务器共同工作的具体信息参见如下 URL：
http://www.mdaenon.com/helpdesk/

其它信息

- 如果您发送邮件到“procnow@mydomain.com”，MDaemon 将会产生 procnow.sem 文件。因此，您不能使用“procnow”作为您账户之一的 email 邮箱。
- 在 LAN DOMAINS 标签中所列的邮件到域保存在 LOCALQ 目录下的 LNDOMAIN。
- 如果您发邮件到 gateaddress@mydomain.com，MDaemon 将发送您一个邮件，告诉您 MDaemon 产生的域名和 IP 地址。如果您在自动拨号时想知道您电脑的 IP 地址，这是非常有用的。

备注：

我们力求翻译的准确性，因为版本的不断更新，请参照最新的英文版用户手册，网站：www.altn.com 。您可以从www.altn.cn 下载最新的中文版软件。

如果您发现以上译文中存在的任何问题，请将您的宝贵意见及时反馈给我们。
邮件地址：support@altn.cn

详情请登陆 中文：http://www.altn.cn 英文：http://www.altn.com